ICE Desktop User Guide

Product guide for prerelease

Copyright © 2024, Instant Connect Software, LLC. All rights reserved.

Document version 1841, produced on Friday, September 06, 2024.

main 90adc8bf40040649230176bbdd465f6261a2d8e0

ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. STA GROUP DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL INSTANT CONNECT LLC OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF STA GROUP OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks mentioned in this document are the properties of their respective owners.

Contents

List of Tables

1 Document History

Publication Date	Product Release	Notes
May 28, 2024	3.5.1	Updated supported options for translation providers at Settings > Organization > Linguistic services, including the addition of 'AWS Web Services', as well as a Disconnected Cognitive Services option, i.e., 'Azure Cognitive Services (Containers)'.
April 15, 2024	3.5.0	Many updates to make document current with release 3.5.0. Some highlights include the Ops Log, Translations, and Group Admin features, as well as the new 'dark' UI design. In 'Archived Recordings', added note that the feature is unavailable for a channel if Rallypoint is disabled.
October 27, 2023	3.4.0	Added *'Rallypoints'*, *'Patch Servers'*, and *'Static Reflectors'* sections.
September 20, 2023	3.4.0	Added 'Web client feature limitations' section. Added 'Appendix A: Add firewall rule for ICE Desktop to receive audio' section.
July 24, 2023	3.3.0	UI redesigned, so many updates to screenshots. Added web client option. Added 'Archived recordings' section.
December 1, 2022	3.2.0	Release updates. For ISSIG support, added 'ISSI Gateways' and 'Radio Systems' sections. For tactical mode, added 'Tactical License Blocks'. Added channel colors and display sizes. Added channel cross muting. Added sample .CSV files for bulk upload of channels and people.
September 26, 2022	3.1.2	Release updates. Added command-line switches for install. Added admin view/update/delete info for channels and people.
March 15, 2022	3.1.0	Document created.

2 Introduction

ICE Desktop™ is a PC-based application that enables your company to manage Push-to-Talk (PTT) communications across your organization via mobile devices, radios, IP phones, and PCs. This application supports two modes of operation: Tactical and Enterprise.

A standalone component of Instant Connect, ICE Desktop provides Push-to-Talk, intercom channels, GPS based location tracking, user monitoring, and channel management through an intuitive user interface that runs on a client PC. It also enables management of Instant Connect resources and control of Instant Connect missions packages that provide Push-to-Talk channels without a connection to any server infrastructure.

Instant Connect turns your PC into a communication hub that allows you to communicate across your company's communication devices individually and in talk groups. A user can sign in from any location with network connectivity and manage activities for a group of mobile (PTT) users.

This document introduces ICE Desktop and provides information about installation, operation, and related activities.

3 Key Features

Instant Connect is a leading open standards-based communications platform that seamlessly links mobile clients, radios, enterprise telephony, and centralized dispatch in a single, secure, device-independent environment. The ICE Desktop software includes the following features:

Dashboard The Dashboard screen is used for enterprise authentication and is the user interface for all active channels.

Missions Missions are an easy way to create and manage channels (talk groups) and participate in communication with other users across your organization from your PC. Each mission contains a group of channels that provide seamless (PTT) communication via multiple devices.** **

Channels Channels are the talkgroups that can be assigned to a group of people and/or contacts designed to have secure communication across your organization via multiple media devices. Channels can be created, managed, and shared centrally by your IT department or by individual users to meet your organization's communication requirements.

PTT Communication Push-to-talk allows instant communication to one or more people (talkgroups) via other mobile devices, radios, phones, and PCs with a push of a button.

Monitor Channels Allows a user to monitor communication across multiple channels simultaneously, join existing active communications, initiate a new channel, view information for users on a channel, and locate users on a map.

Intercom Channel Allows a user to create a channel with one or more users. This feature enables your mobile device to communicate directly with other PC and mobile device users.

Group PTT Provides the ability for PTT on a shared channel with other clients. The transmission can be heard by all other clients or resources on the shared channel.

Group PTT Simulcast Provides the ability to talk on multiple channels at the same time by selecting them before using PTT.

Secure Communications Provide the ability to encrypt PTT communications on a channel. Audio is encrypted with AES 256 and client connections are secured with TLS 1.2.

Channel Mute Provide the ability to mute incoming audio per channel.

Talker ID Displays the name of the Instant Connect user talking on a channel.

Channel Participants (Per Channel) Displays the list of participants on a channel.

GPS Mapping (Per Channel) The ability to provide location updates on each GPS enabled device. Clients use the built-in maps to display the location of each client on a channel.

Talker History Displays PTT transmit and receive history per channel.

Channel Volume Increases or decreases volume of incoming audio on a channel.

Map Provides real-time visual location tracking information of all participating members across your organization. Multiple contacts or individuals can be located on the mapping application.

Mission Sharing Provides users the ability to share a mission with other users via a QR code or file that can be read from internal or external storage devices.

Rallypoints Enable PTT communication from devices that are outside of your network and have internet access. Rallypoints enable the conversion of multicast packets to unicast, allowing multicast communications to be routed over unicast network segments and over the internet.

Unicast Unicast enabled PTT communications from devices to Rallypoints are forwarded to other connected devices or Rallypoints with clients that are using the same channels.

Multicast Multicast enabled PTT communication from devices inside your network.

Channel (PTT) Audio Replay Each channel on an ICE client has the ability to replay audio that is received within a configured time frame.

IP Telephony Ability for the user to Make, Receive phone calls from the mobile client. **These users can also join an ICE channel to communicate with other users via PTT**

Private Call 1:1 Ability for the user to Make, Receive private full-duplex call between ICE mobile clients and/or ICE Desktop clients.

Instant Messaging Users can send and receive instant messages via conversations, which are chat groups based on either a channel or a selected group of users.

Patching Advanced Desktop Users have the ability to manage patches of multiple channels. The users can Create, Modify and Delete patches on the ICE system.

Notifications Desktop users have the ability to send Alert notifications on a channel that will be received by all users assigned to the channel.

Workflow Automation Advanced Desktop Users provisioned with the Workflow Automation administrator permission will have the ability to manage workflows. Workflow Automation allows the user to configure rules that will dynamically create alerts, channels, and user channel assignments. Configuration includes how the rules are triggered, e.g., a user entering or leaving a geofence boundary, date/time, Webhook.

Transmit Priority Transmit priority allows higher priority users to preempt lower priority users on the same channel. Users are assigned a transmit priority, which is a 5-level range from 'highest' to 'lowest'. The ICE desktop and mobile clients display a notification to users when they are being preempted.

4 Related Documentation

Instant Connect documentation is available at the following URL: *https://support.instantconnectnow.com*

Access to the Instant Connect Enterprise support portal requires an account to be created. To create a support portal account:

1. Open a browser to *https://support.instantconnectnow.com*
2. Click on the ***Create your Instant Connect Portal Account*** link
3. Fill out the form with your information and click Submit

A portal access account will be created and an email will be sent with your access information.

5 PC client

ICE Desktop is available in the following versions:

- NSIS .EXE (Windows)
- .MSI (Windows)
- Web (Web Browser: Chrome, Edge, Firefox, etc)
- MacOS

- AppImage (Linux)
- Snap (Linux)

> **Note:** Only the .EXE, .MSI, and Web versions are available on the Support Portal. If you are interested in the other verions, contact Instant Connect Support.)

5.1 Hardware and Software Requirements

A client PC on which you install and operate ICE Desktop must meet the following minimum requirements:

- Windows 10 Enterprise 64-bit operating system (or newer)
- 4 CPU cores
- 8GB RAM
- 1GB of free HDD space

One instance of ICE Desktop can be open on a client PC at a time. Any number of Instant Connect users can use the same ICE Desktop on a client PC, but not concurrently.

5.2 Install ICE Desktop

> **Note:**
>
> - The prior version of ICE Desktop does *not* need to be uninstalled prior to installing the latest version.
> - This section covers the most common installation method, i.e., .EXE. If in need of assistance to install any version of ICE Desktop, please contact Instant Connect Support.

This section describes how to install ICE Desktop on a client PC. Before you begin, ensure that the client PC meets the requirements described in the 'Client PC Hardware and Software Requirements' section above.

5.2.1 Download the ICE Desktop Installer

Instant Connect Desktop Installer is available at the following URL:

https://support.instantconnectnow.com/s/downloads

1. Open the 'Instant Connect Enterprise Software' folder.
2. Open the most recent 'ICE' release folder.

3. Download the '[RELEASE] ICE Desktop Installer EXE' file. The downloaded zip folder is named 'ICE_Desktop_NSIS'.
4. Unzip the folder and open it to see the .

5.2.2 Install ICE Desktop

1. Open the 'Instant Connect Setup' .EXE file.
2. Select whether to install for all users or only the current user
3. Select 'Next'.
4. Confirm the install location, by default it is:
    - All users: `C:\\Program Files\Instant Connect`
    - Current user: `C:\\Users\<username>\AppData\Local\Programs\Instant Connect`
5. Select 'Install'.
6. Watch the 'Installing' progress bar reach completion.
7. Select 'Finish'.
8. ICE Desktop is now installed to the PC.

5.2.2.1 Command-line switches (.EXE)

> **Note:** No restart is required.

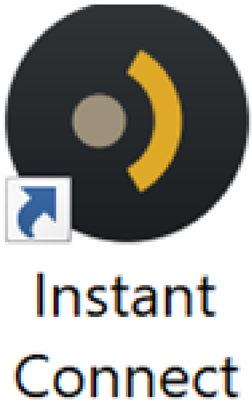
If you are installing ICE Desktop (.EXE) via command-line, the following switches are available:

- Silent installation: `/S`
- Installation for all users: `/ALLUSERS=1`

5.3 Start ICE Desktop

The following guidelines apply:

- You can run one instance of ICE Desktop on a client PC at a time.
- Before you can log in to ICE Desktop on a client PC on which another user is already logged in to ICE Desktop, the other user must exit ICE Desktop.
- Any number of Instant Connect users can use the same ICE Desktop application, but not concurrently.



To start ICE Desktop, double-click the **Instant Connect** icon on your Windows desktop.

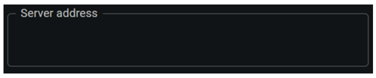
Alternatively, you can open the ICE Desktop file in the default installation directory:

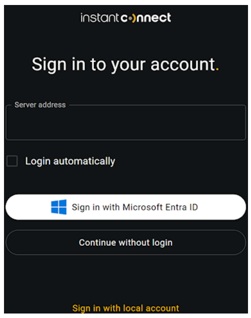
- All users: `C:\\Program Files\Instant Connect`
- Current user: `C:\\Users\<username>\AppData\Local\Programs\Instant Connect`

The **ICE Desktop** loading displays while the application starts up.

When ICE Desktop start up is completed the Dashboard will be displayed. All Missions that have been loaded will be displayed in the channel list. At this point you can run the client in Tactical mode and use the Missions and Channels that have been loaded.

5.4 Login to ICE Desktop

1. In **Server address,** enter the URL of your ICE Server. 

2. Tap the **Continue** button.
3. Use one of the three options listed below to sign in. 

   1. Tap **Sign in with Microsoft Entra ID** (Enterprise mode) to open the Microsoft login window. Select your account and then your organization’s instructions. This option appears only if enabled by your organization.

2. Tap **Sign in with local account** (Enterprise mode): Enter your username and password, then select 'Sign in'.
   - **Username:** Your ICE account user name, which was assigned by your ICE administrator.
   - **Password:** Your ICE account password, which was created by your ICE administrator. Passwords must be a minimum of eight characters in length and must contain at least one digit (0-9).
3. Tap **Continue without login** (Tactical mode): Please see the **ICE Desktop Tactical Mode** section further down in this document.

4. After your credentials are validated, the ICE Desktop dashboard opens.

5.5 Exit ICE Desktop

Exiting ICE Desktop logs you out of the application and closes the application.

To exit ICE Desktop, perform either of these actions, and then click **Yes** to confirm:

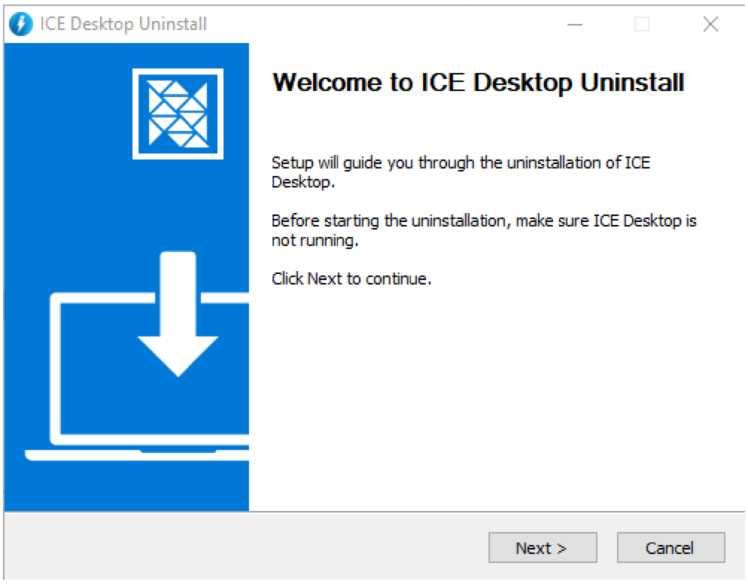
- Choose **File** > **Close**.
- Click the **X** icon at the top right of the main window .

5.6 Uninstalling ICE Desktop

> **Note:** Uninstalling ICE Desktop from a client PC removes the application from the PC.

To uninstall the ICE Desktop from a client PC:

1. From Windows, got to Settings > Apps > Apps & Features.
2. Scroll down the list of apps to find 'Instant Connect'.
3. Select 'Instant Connect'
4. Select '_Uninstall'.
5. Again select 'Uninstall'



6. From the resulting uninstall wizard, select 'Next'.
7. Select 'Finish'.
8. The ICE Desktop app is uninstalled from the PC.

6 Web client

ICE Desktop is available as a web application accessed via your web browser. Most of the same features and functions are available as the PC client.

The web client option is enabled via ICE Server configuration. Please see the *ICE Server Installation Guide* or *ICE Server Upgrade Guide* for more information.

To access the ICE Desktop web client, enter the URL or IP address configured for ICE Server. No installation is required.

6.1 Web client feature limitations

The web client has the following feature limitations in comparison to the PC client:

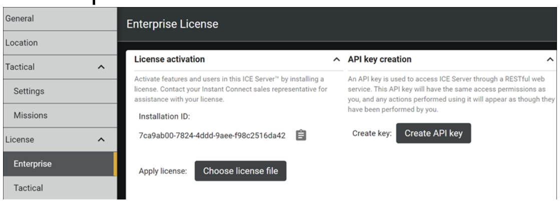
- Hot keys (keyboard shortcuts): Unavailable due to security reasons, i.e., a web page cannot monitor key-press events when the user does not have the window in focus.
- Audio steering: References to mic and speaker device selection are unavailable in the web client. These selections are made via browser settings (in a manner specific to each browser).
- Multicast audio: Web browsers do not support transmitting or receiving IGMP multicast traffic. Channels must be configured to use a Rallypoint in order to work. Otherwise they will display a "Channel not available on web" message.

- Gravatars: The web client will only display a user's initials as their avatar.
- MELPe Codec: Channels configured to use this codec will not function on the web and will appear with the "Channel not available on web" message.
- FIPS 140-2 (Wolf SSL): All SSL connections utilize the browser's internal crypto engine for security. Customers interested in FIPS-compliant security should choose a FIPS-compliant browser.
- App sounds: Some browsers will squelch audio (like ring tones) produced by a web application when the browser window is minimized or in the background.
- Web browsers: The web client has been tested and qualified for use on these browsers:
  - Chrome: 114 and newer for Windows
  - Edge: 114 and newer for Windows
- Mobile browsers: The web client is not supported on mobile web browsers (iOS, Android).
- Unsecured HTTP: The web client will only work when hosted from a server using a secured connection (HTTPS). The ICE Server must be configured with a fully-qualified domain name and accompanying SSL certificate.
- Rallypoint: ICE Desktop for Web requires the following conditions to be met in order for a channel to operate within a browser:
  - Rallypoint versions 1.236 and newer.
  - Rallypoints records in ICE Desktop must be configured to use port 7443 (under Settings > Rallypoints). The referenced Rallypoint must then be configured to enable web socket connections on port 8443 and accept client connections on 7443. (Default Rallypoints installed inside ICE Server at the time of install are automatically configured this way.)
- Rallypoint failover: The web client does not support Rallypoint failover. When a channel is configured to use a Rallypoint with multiple ingress addresses, the web client will only connect to the first address configured, even if that Rallypoint is unreachable.
- Certificates: The root CA certificate AND every intermediate certificate in the signing chain must be installed and trusted by the web browser.
  - Because the Rallypoint acts as a server to which the browser connects, and a secured HTTPS connection is required, then the Rallypoint must present a trusted server identity certificate to the browser, and so the Rallypoint must be configured with a certificate and private key.
  - For a Rallypoint deployed inside the ICE Server (at time of installation), the ingress server identity certificate and key will be used by the Rallypoint. The server identity certificate is supplied as the first certificate in the PEM bundle entered in the ICE OS Configuration Wizard (on the 'TLS Certs' screen).
  - When using a widely accepted ingress certificate (that is, one issued by a common, commercial certificate authority) this should work out of the box.

7 ICE Desktop Licensing & Organization

The ICE Desktop license is controlled by the Instant Connect Enterprise server in Enterprise mode. When you start ICE Desktop, the Instant Connect Enterprise Server checks for an available license and either allows or denies your log in based on license availability.

7.1 Enterprise Mode Licensing

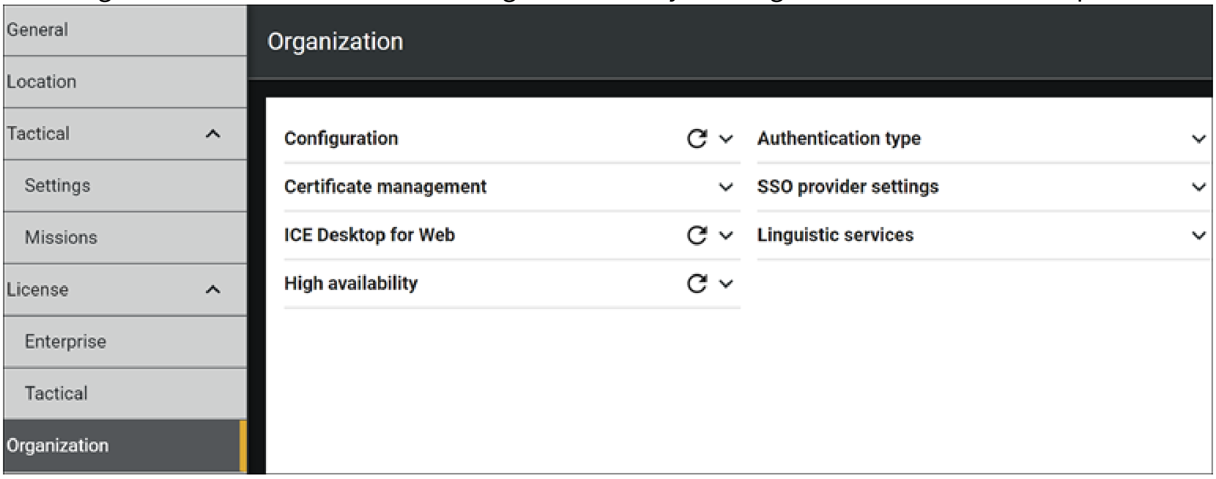
Enterprise licensing is maintained by your Instant Connect Enterprise administrator. The Instant Connect Server contains the license file pool for the number of desktop clients allowed to be logged in simultaneously. A license file will be consumed from the pool of licenses on a successful login by a user on a desktop client. The license will be returned to the pool of available licenses when the user logs out. 

7.2 Tactical Mode Licensing

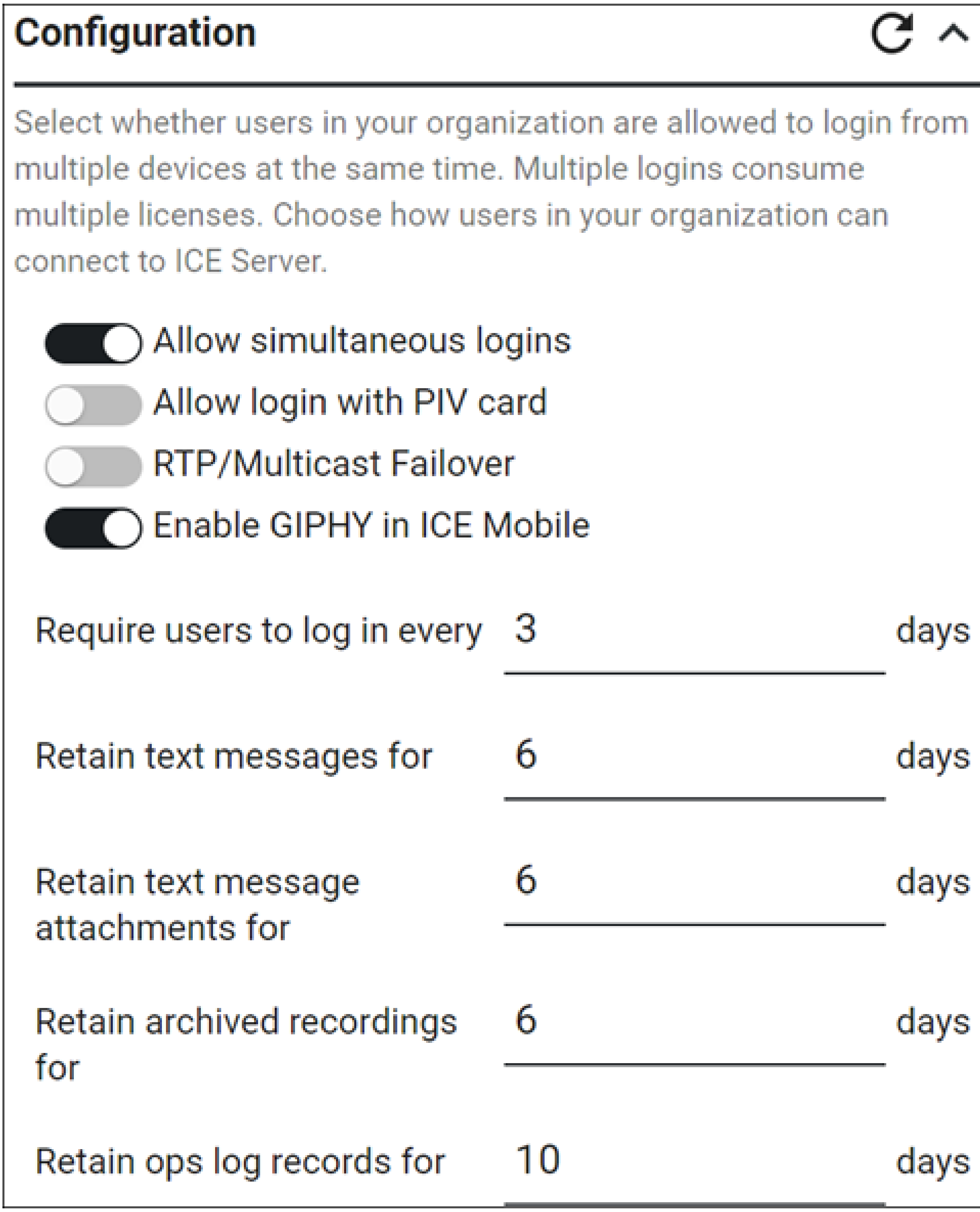
Unlicensed software can communicate via push to talk for up to 3 seconds at a time. Please see the *'Tactical License Activation'* section below for more information. To obtain a valid **ICE Desktop** license contact your sales associate or **Instant Connect** support located at **https://support.instantconnectnow.com**.

7.3 Organization

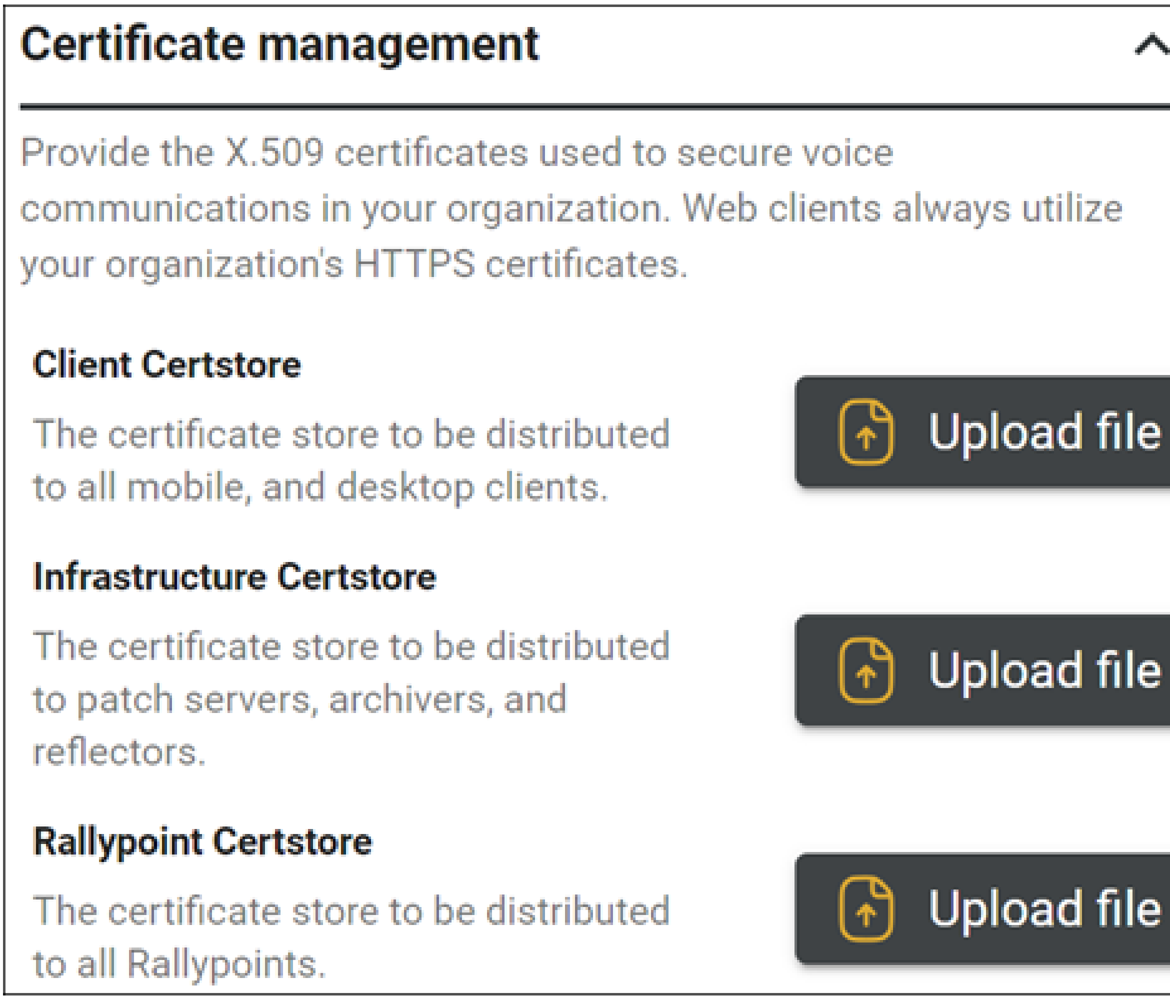
The Organization screen allows configuration of your organization's ICE Desktop features.



Configuration:

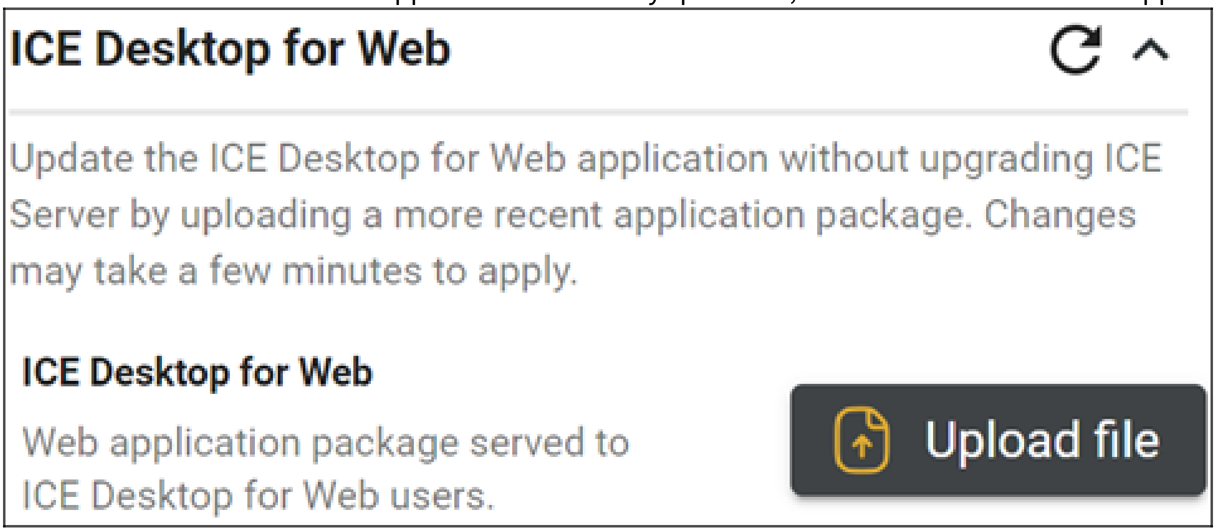


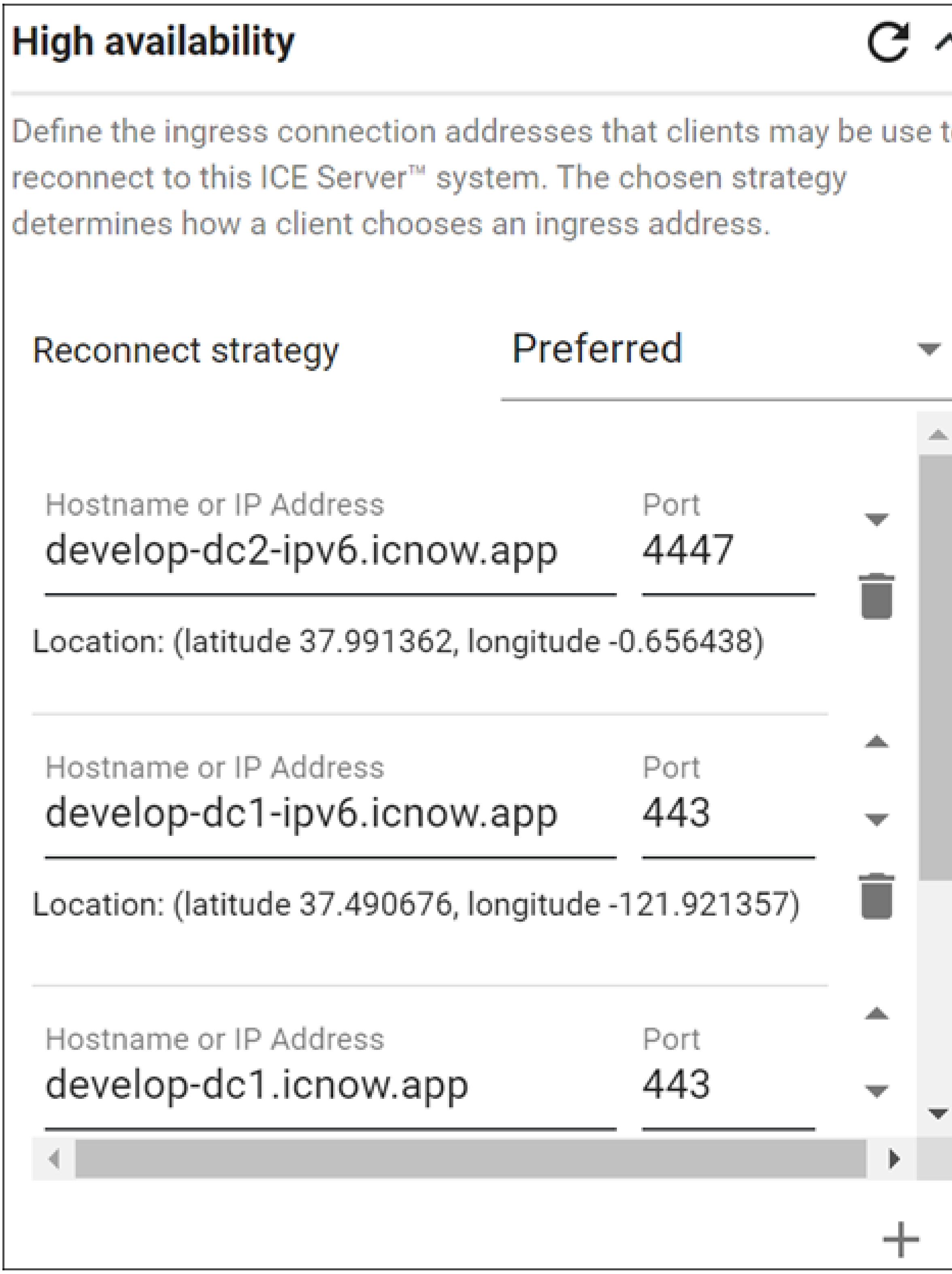
Certificate management: Please see the ***ICE Private Certificate Stores*** document for more on certifi-



cate management.

ICE Desktop for Web: Allows for updating the ICE Desktop web client. The update files are available via the Instant Connect Support Portal. For any questions, contact Instant Connect Support.

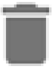


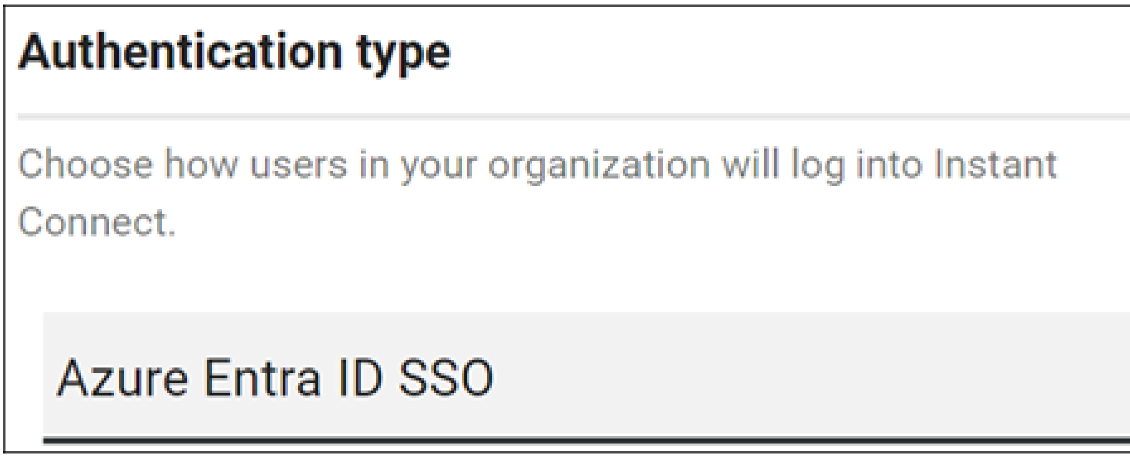


High availability:

- Select a reconnect strategy:

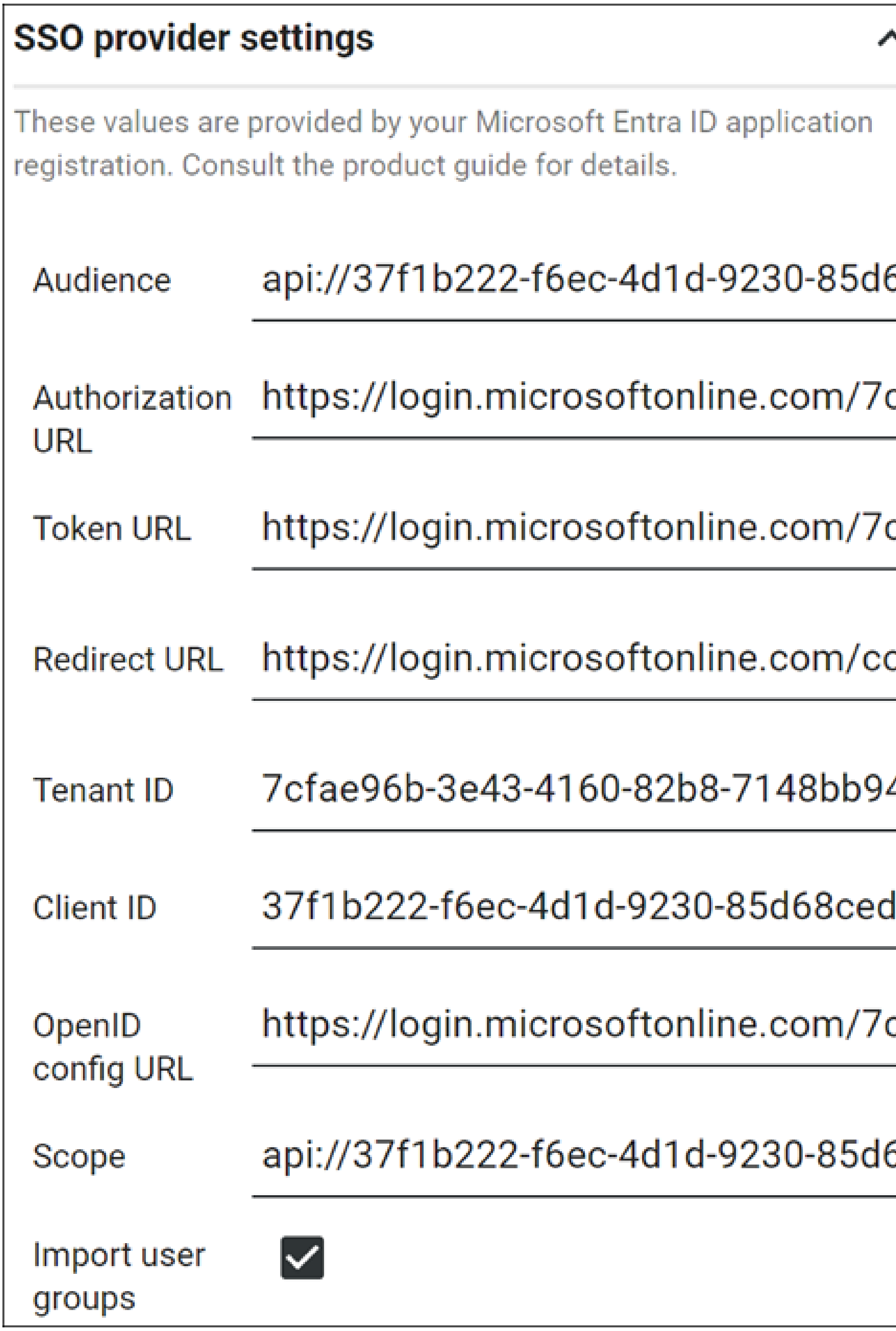
- Preferred
- Nearest
- Random
- Identity

- Add a host/IP address by selecting the + button.
- Delete a host/IP address by selecting the  button.

Authentication type: 

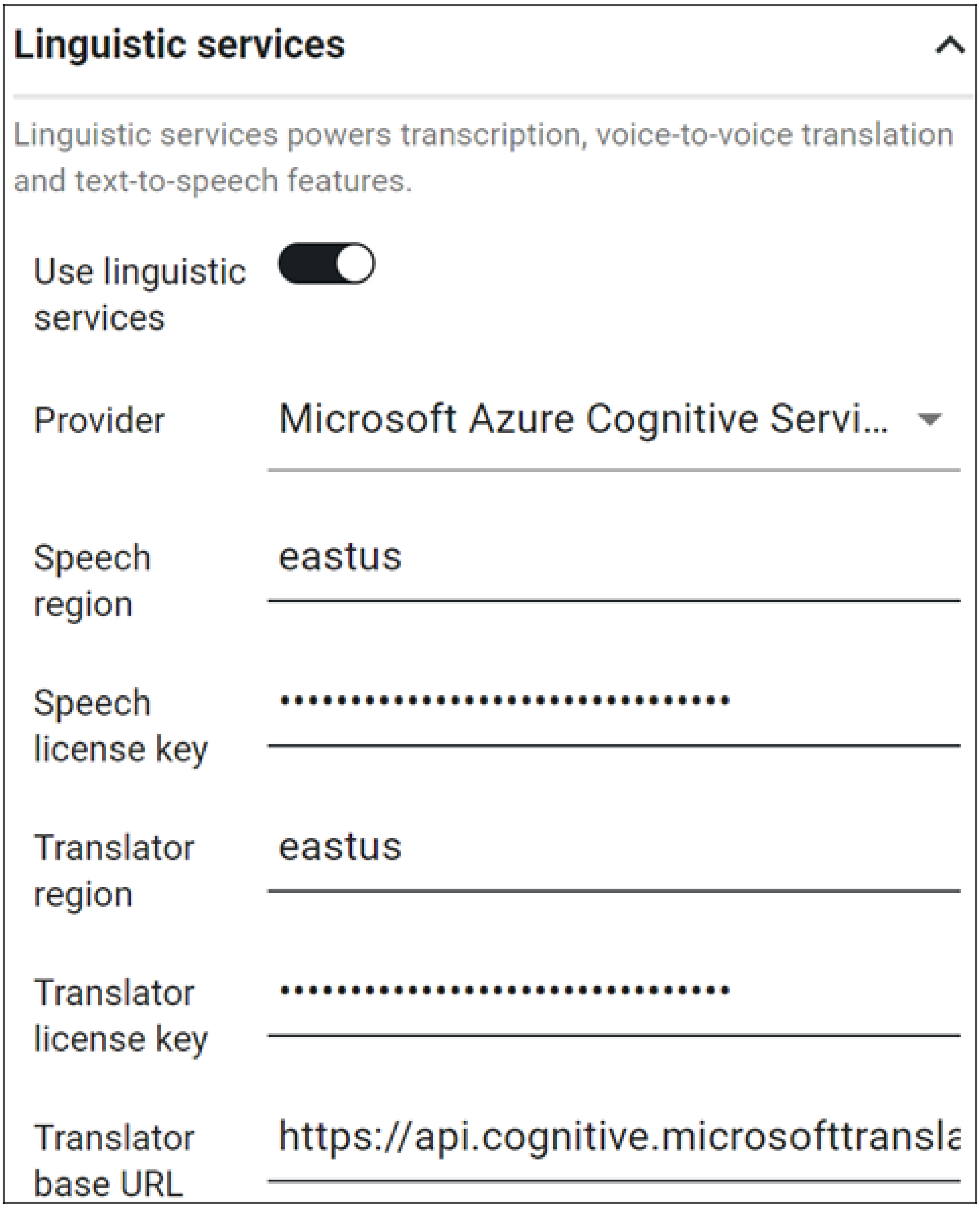
- Select the user login method from:
  - User name and password
  - LDAP: Please see the ***LDAP Configuration on ICE Server*** document for more on configuring LDAP.
  - Azure Entra ID SSO

SSO provider settings:



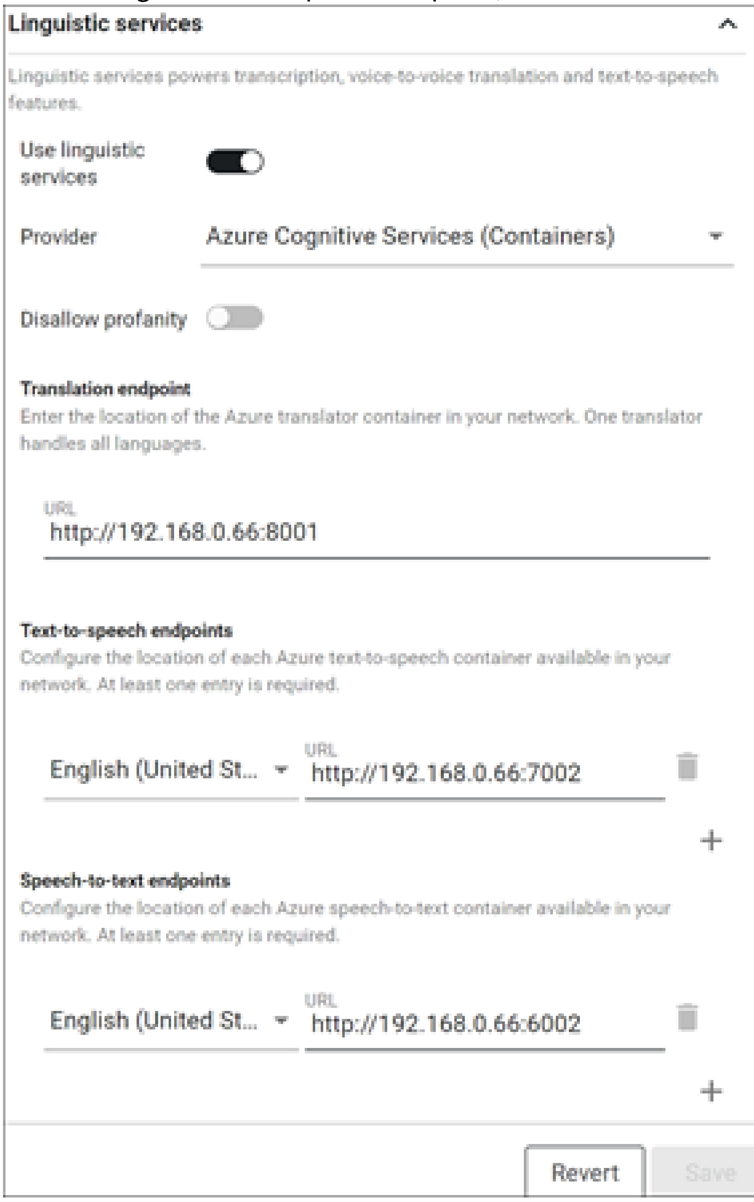
7.3.1 Linguistic Services

> **Note:**
>
> - Only ***one*** provider option can be configured at a time. If you select a new provider option and save it, then any prior configuration done on another provider option is ***overwritten***. On selecting that prior provider option, the configuration fields will have reset to default-/blank.
> - Some provider configurations require your organization's linguistic services license, speech, and/or access keys. Instant Connect Support does not know or have access to these keys and so ***cannot help with requests to provide or recover those keys***.



- For the **Translations** feature, select from the following providers:
  - Instant Connect (Transcript only)
  - Azure Cognitive Services
  - Azure Cognitive Services (Private Cloud)
  - Azure Cognitive Services (Containers)
  - Amazon Web Services

7.3.1.1 Disconnected Cognitive Services There must be corresponding text-to-speech and speech-to-text endpoints for each language, e.g., if there is an 'English' text-to-speech endpoint, then there also will be an 'English' speech-to-text endpoint.

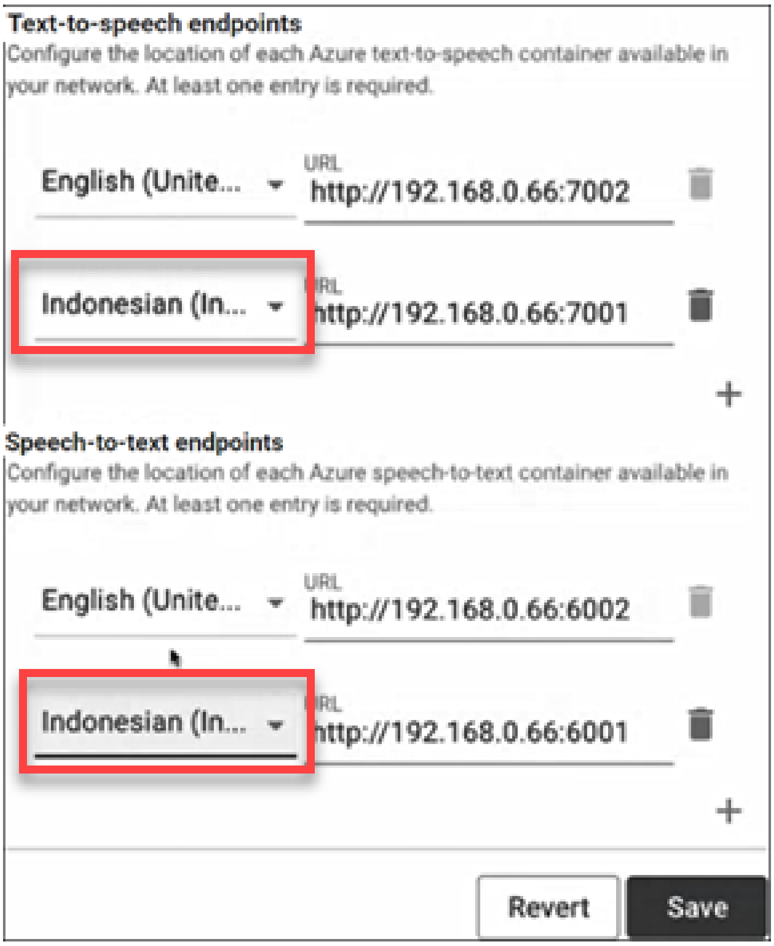


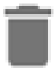
7.3.1.1.1 Create endpoints

1. Got to *Settings* > *Organization* > *Linguistic services*.
2. **Use linguistic services:** Toggle on.
3. **Provider:** Select 'Azure Cognitive Services (Containers)'.
4. **Disallow profanity:** Toggle on to have the service automatically exclude profanity. The original language transcript the profanity is replaced with a string of *****, while in translated

transcripts the profanity is replaced with the term 'profanity'.
5. **Translation endpoint:** Specify the URL of the Azure translator container in your network.
6. **Text-to-speech endpoints:** Specify the language and URL of the text-to-speech container in your network.
7. **Speech-to-text endpoints:** Specify the language and URL of the speech-to-text container in your network.
8. Select '+' to add additional endpoints.
9. Select 'Save'.

7.3.1.1.2 Update endpoints If an endpoint's language is updated, then the corresponding endpoint automatically updates to the same language. In the example below there are 'German' text-to-speech and speech-to-text endpoints.

When one of the 'German' endpoints is updated to 'Indonesian', the other 'German' endpoint automatically updates to 'Indonesian', too. 

7.3.1.1.3 Delete endpoints Delete an endpoint by selecting the the  button. If an endpoint (text-to-speech or speech-to-text) is deleted, then the corresponding endpoint is automatically deleted, too.

8 ICE Desktop Enterprise Mode

After you log in to Instant Connect Enterprise, the ICE Desktop window displays. The following figure describes this window.

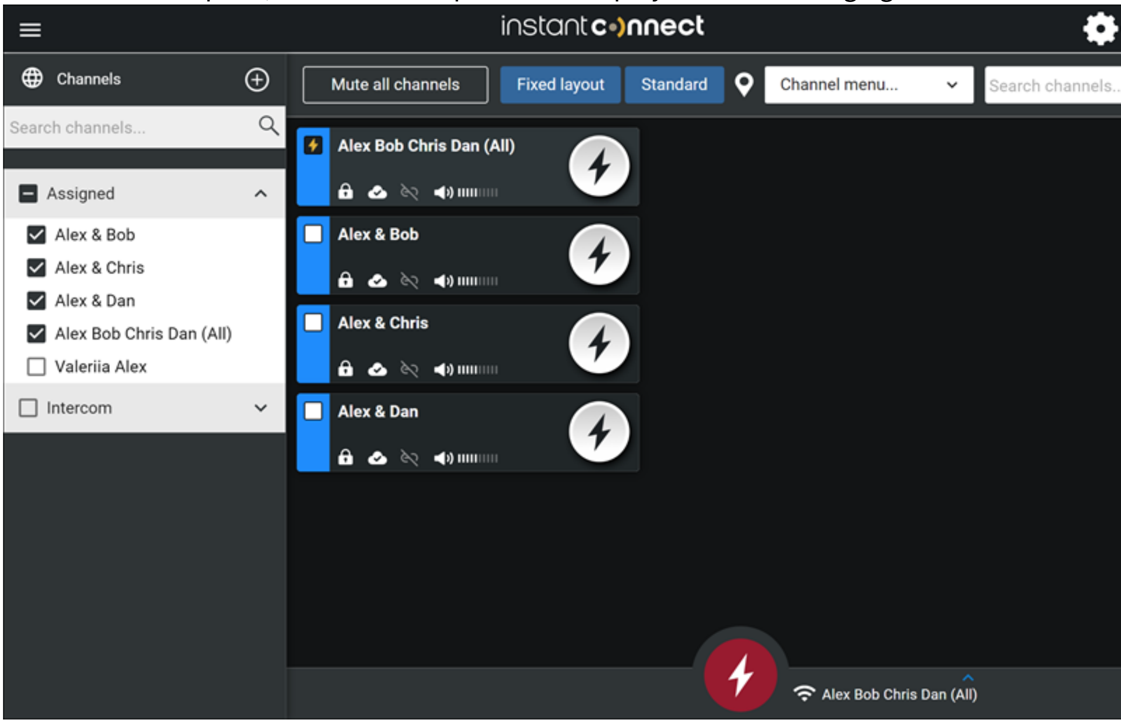
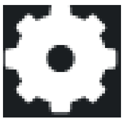
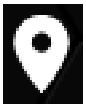
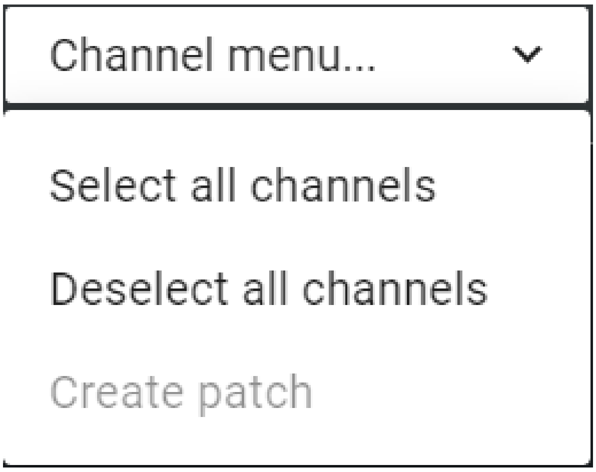
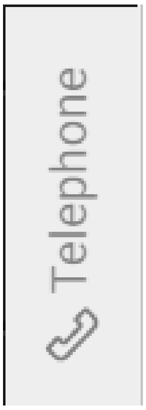
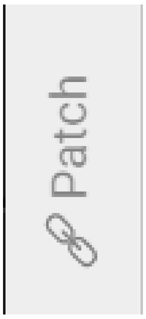
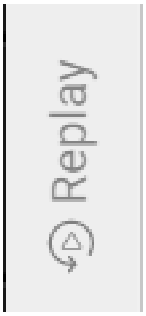
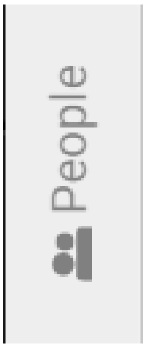
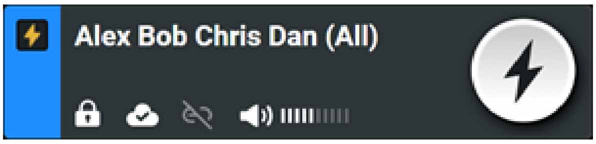


Table 2: Desktop Icon Descriptions

Icon	Description
	**Channel List**–Opens or closes the Channel List
	**Settings**–Opens the Settings window
	**Notifications**– Opens the Notifications list
	**Account**–Provides access to your Instant Connect Enterprise account information

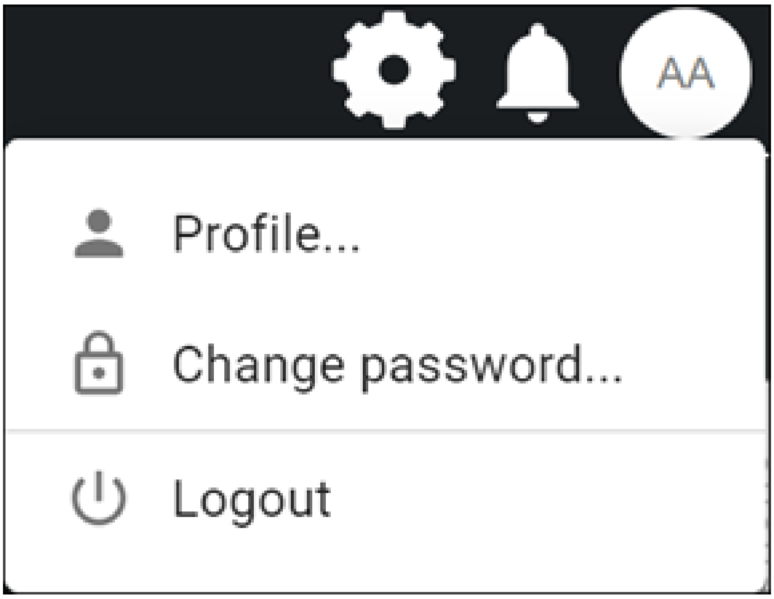
Icon	Description
	**Channel Mute**–Mute / Unmute all channels
	**Fixed Layout**–Sets channel cards to a fixed grid layout in the Dashboard**Free Layout**–Allows the user move channel card to any location in the Dashboard
	Select from standard, compact, and tiny channel display sizes
	**Map**–Opens the map in a new window
	**Channel Menu**–Opens the channel actions drop-down menu for Select / Deselect channels
	**Channel Search**–Updates Channel cards to display channels that include string of characters that you enter

Icon	Description
	**Telephone**–Opens the Telephone tab for making calls, receiving calls, call history
	**Messaging**–Opens the Messaging tab to send and receive instant messages via conversations, which are chat groups based on either a channel or a selected group of users.
	**Patch**-Opens the Patch tab to Create, Modify and Delete patches. Only displayed if the user is provisioned with the Patch agent permission.

Icon	Description
	**Replay**–Opens the Audio Instant Replay tab for replaying audio transmitted and received on configured channels
	**People**–Opens the People tab to view the users active and users provisioned for each channel
	**Channels**-Active channels that are associated with your user account or active Missions

8.1 Account Menu

The Account menu provides options for logging out and managing your Instant Connect Enterprise account information. To access the Account menu, click the Account icon on the Dashboard screen.

The following figure describes the Account menu. 

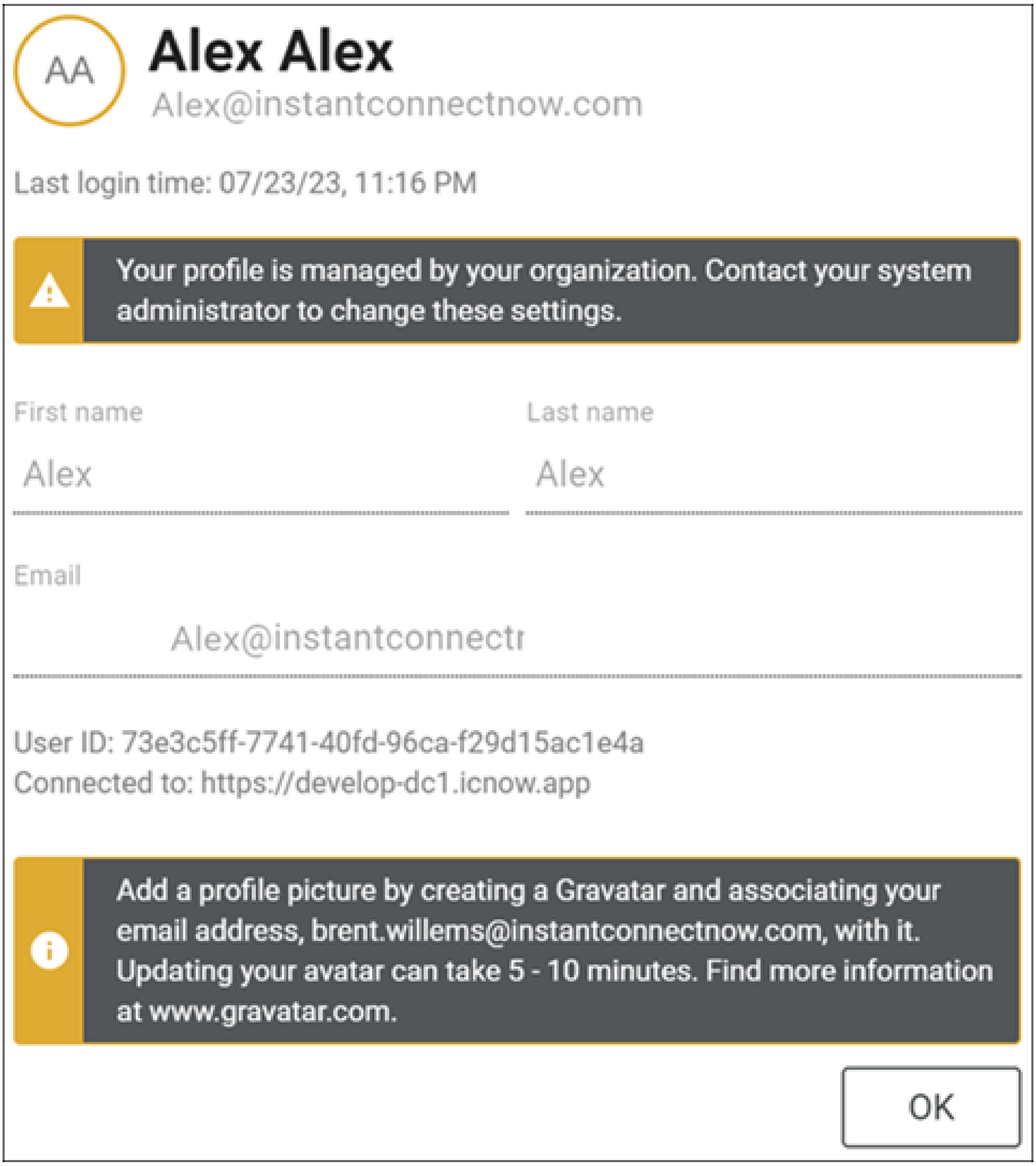

AA
Alex Alex
Alex@instantconnectnow.com
Last login time: 07/23/23, 11:16 PM
Your profile is managed by your organization. Contact your system administrator to change these settings.
First name
Alex
Last name
Alex
Email
Alex@instantconnectr
User ID: 73e3c5ff-7741-40fd-96ca-f29d15ac1e4a
Connected to: https://develop-dc1.icnow.app
Add a profile picture by creating a Gravatar and associating your email address, brent.willems@instantconnectnow.com, with it. Updating your avatar can take 5 - 10 minutes. Find more information at www.gravatar.com.
OK

Table 3: Account Icon Descriptions

Icon	Description
	**Account**–Opens the Account menu.
	**Profile**–Displays your Instant Connect Enterprise account profile window. A profile picture can be added via Gravatar by using your email address. See the blue message box at the bottom of the screen. Visit (http://www.gravatar.com/) for more information.
	**Change Password**–Changes your Instant Connect Enterprise account password. Passwords must be a minimum of eight characters in length and must contain at least one digit (0-9).
	**Logout**–Log out of your Instant Connect Enterprise account.
	**Account information**–Your Instant Connect Enterprise User name and email address.
First name / Last name	Full name of the user account
Email	Email address that is associated with your user account.
User ID	User ID is the unique identifier for this user account. It is used by the system components to identify this user account and cannot be changed or edited.
Cancel	Exits the account profile window without saving any changes.

Icon	Description
Save	Saves changes to the account profile and exits the window

8.2 Channels

A channel is a group of people and contacts. Channels organize and secure communication across your organization via multiple communication devices.

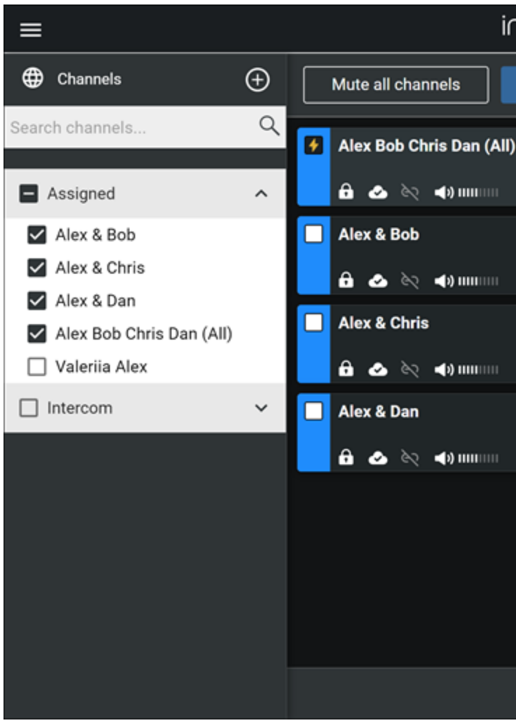
Assigned Channels associated with your Instant Connect Enterprise account are centrally managed by your organization IT department.

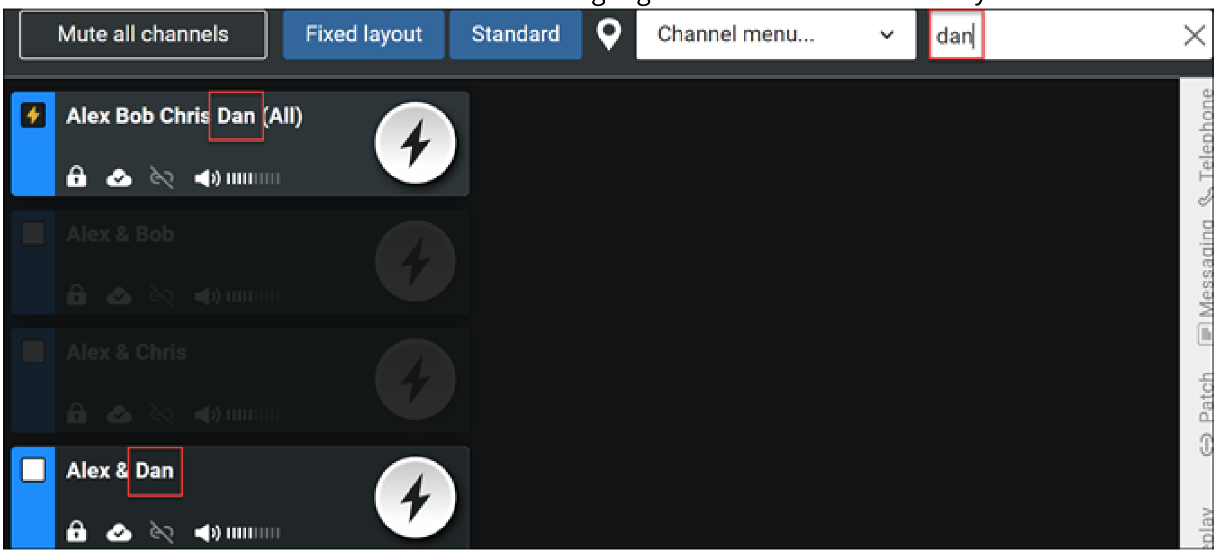
Intercom Channels are Ad Hoc channels created by users to communicate directly with one or more users. These channels are not managed by the ICE Server administrators.

Mission Channels are created from a Mission configured on your device or by loading a Mission file or scanning a Mission QR Code. See Tactical Mode section.

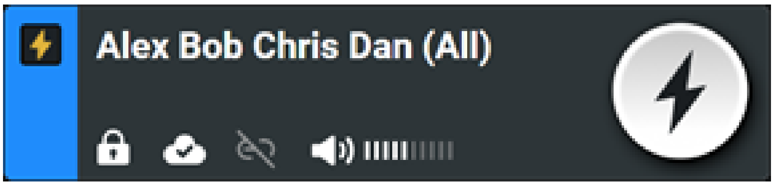
8.2.1 Accessing Channels

The Dashboard screen shows all channels that are activated on your device. To activate channels or to see the list of available channels for your device Go to **Channels** in the menu.

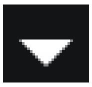
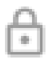
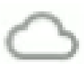
The Dashboard screen displays channels that are activated on your device: 

8.2.1.1 Channel Search To search for a specific channel, enter some or all of the channel name in the Channel Search field in the main screen. The channel cards highlight the channels that match your search criteria. 

8.2.2 Using Channels

Each channel displays in a 'card': 

Each channel card consists of the following:

Field	Description
	**Channel Select:** Tap to select/unselect which channels are used in a multi channel simulcast or affected by the 'master' PTT button.
Channel name	The name of the channel, e.g., 'Alex Bob Chris Dan (All)'.
	**Channel PTT:** Press-and-hold to speak via the channel.
	**Channel options dropdown menu:** Displays the options to send audio or text alerts to the channel, modify audio settings, or select a display color for the channel.
	**Channel Encryption:** If displayed, the 'lock' icon indicates that the channel is encrypted.
	**Rallypoint:** If displayed, the 'cloud' icon indicates the channel is using a unicast connection to Rallypoint. If it is not displayed, then the channel is using multicast.

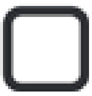
Field	Description
	**Patch:** Indicates if the channel is patched with any other channel.
	**Channel Volume**

The channel card changes color to indicate status/activity:

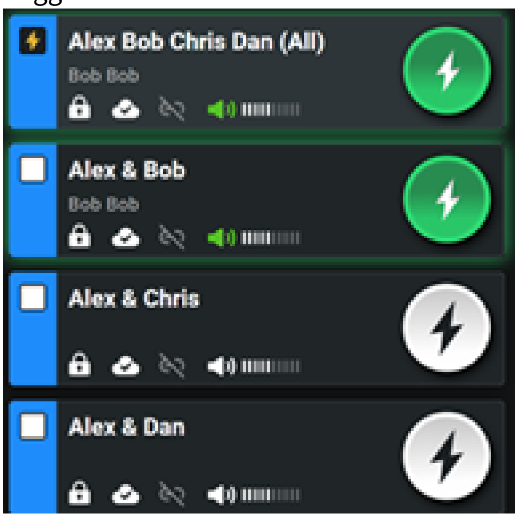
Color	Status
	**Red:** User is sending via the channel (see PTT button).
	**Green:** User is receiving via the channel.
	**Greyed-out:** The channel is muted (see mute button).

8.2.2.1 Single-Channel PTT To talk on a channel, tap and hold its **Channel PTT** button: 

This button turns red, which indicates that the channel is transmitting: 

You can also tap the **Channel Select Box**  to select the channel, the channel select box will change to  indicating the channel is selected, then tap and hold the **Master PTT** button to communicate on the channel.

8.2.2.2 Multiple-Channel PTT To talk on multiple channels at the same time, tap the **Channel Select Box** for each channel that you want selected. The channel select box fills with a check mark which indicates that the channels are selected for PTT. The number of channels that you selected and the **Master PTT** button appear at the bottom of the screen. Tap and hold the **Master PTT** button to communicate on the selected channels.

8.2.2.3 Receiving Audio on a Channel When a channel receives a transmission, the **Channel Mute** turns green. In addition, a green line displays in the channel box for the duration of the incoming transmission. If you see the green button and green line but cannot hear audio, make sure that muting is not toggled on for the channel. The username of the user transmitting will display on the channel card. 

8.2.3 Alert Notifications

Alert Notifications are audio or text alerts sent by a user on a channel and received by all other users on that same channel. You can send audio alerts, which are pre-recorded audio clips, or message alerts, which are preconfigured or custom text.

- Available for Enterprise mode, but not Tactical mode.
- On receiving a notification: a Notification Toast displays, an audio prompt plays, and the Notification Icon counter iterates.
- Notifications persist until deleted by the receiving user via the Notification Panel.

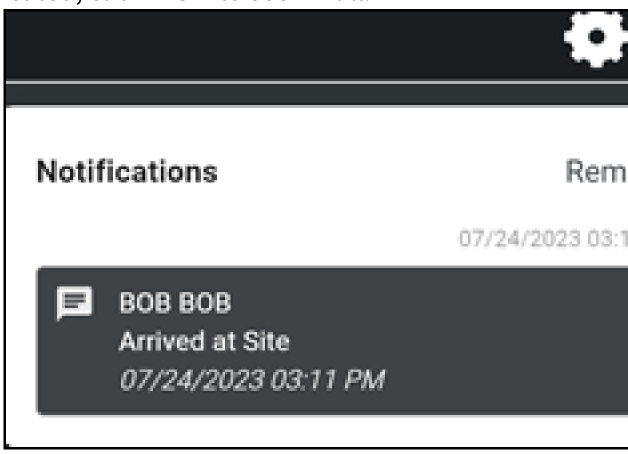
8.2.3.1 Notification Toast

- Displays on receipt of a notification and consists of the sender's name, the header, and a preview of the first line (if there is one).
- After 5 seconds, the toast dismisses itself by sliding off screen. 

8.2.3.2 Notification Icon

- Indicates the number of notifications in the Notification Panel. 
- Click on to see all notifications in the Notification Panel.

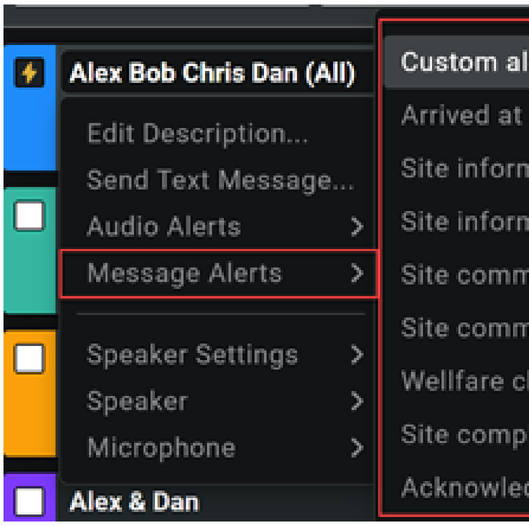
8.2.3.3 Notification Panel

- Displays all notifications. Longer notifications may be truncated, click **View** to see in full.
- Click the garbage can icon next to a notification to delete it. 

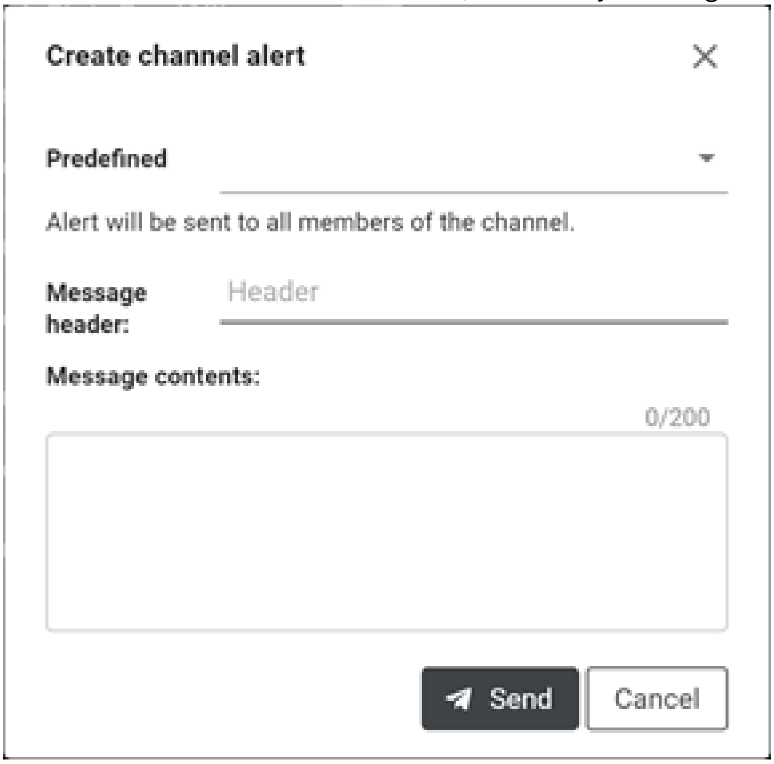
8.2.3.4 Send a Message Alert

1. Select a channel.
2. Select the **Channel options dropdown menu**.
3. Select **Message Alerts**.

4. Select to create a custom alert or select one of the pre-written ones.



5. Review the notification. If desired, edit it by clicking on the header and/or contents.



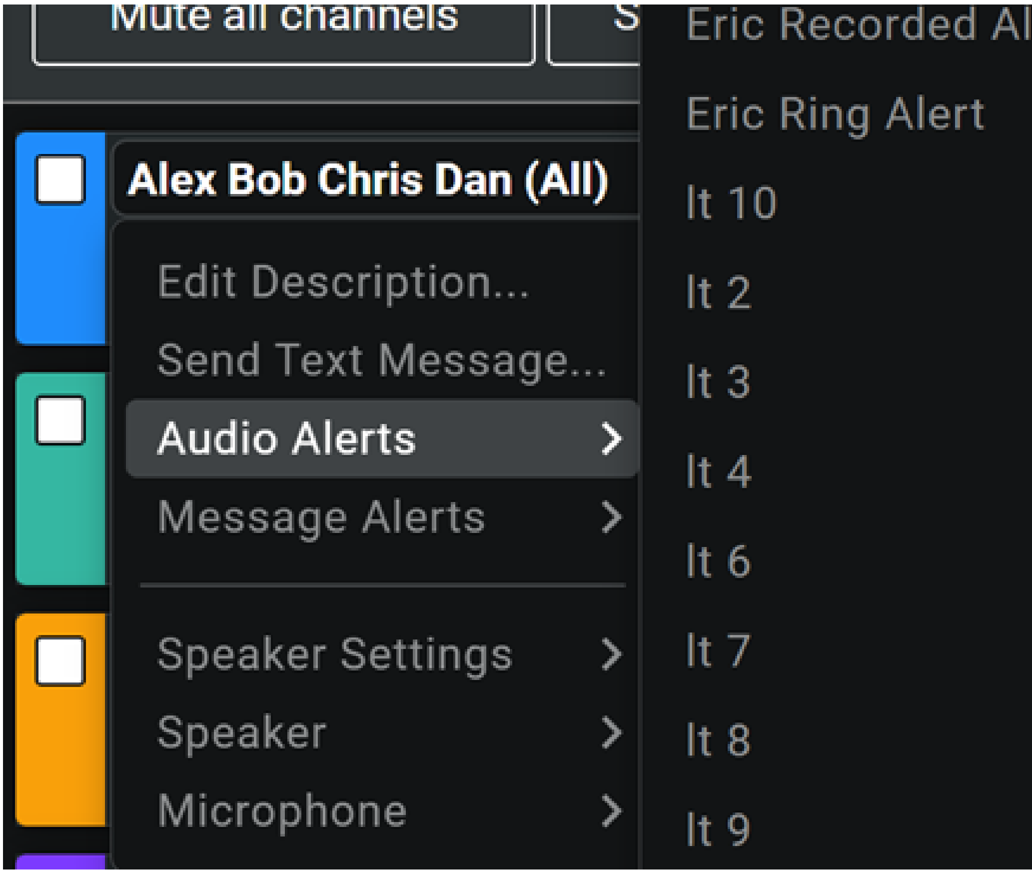
6. Select the **Send** button.

7. A toast displays confirming whether the notification was successfully sent.

8.2.3.5 Send an Audio Alert

1. Select a channel.

2. Select the **Channel options dropdown menu**.
3. Select **Audio Alerts**.



4. Select an alert to send it.
   You will hear the alert and a toast displays confirming whether the notification was successfully sent.

8.2.4 Mute All Channels

To quickly Mute All Channels click the Mute All Channels button. 

All active channels will be muted the Mute All Channels button will change to a Unmute all channels button. 

To restore the channels to the previous mute state click the Unmute all channels button.

8.2.5 Channel Card Layouts

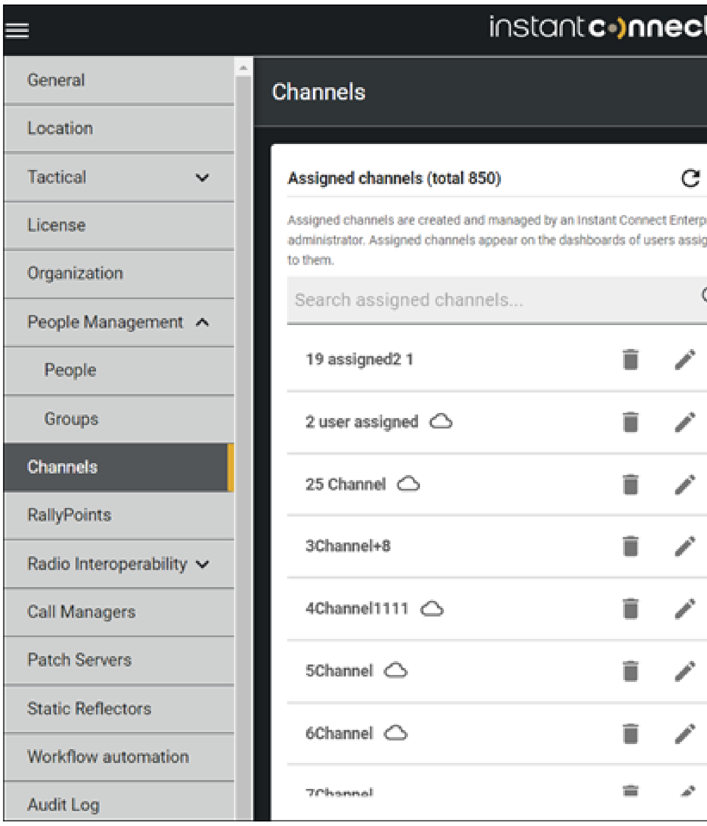
ICE Desktop allows the user to choose how the channel cards will be laid out on the screen.

The user can choose:

1. Fixed grid layout of channel cards in fixed columns without any spaces between the cards.
2. Free grid layout of channel cards in columns that the user can freely choose the column and row for each channel card with spaces in between.

8.2.6 View a channel

1. Navigate to Settings > Channels.



2. Scroll through or search the 'Assigned channels' list.

8.2.7 Add a channels

1. Navigate to Settings > Channels.

> **Note:** The 'channel defaults' screens allow for configuration of the default settings for any new assigned or intercom channels, respectively.

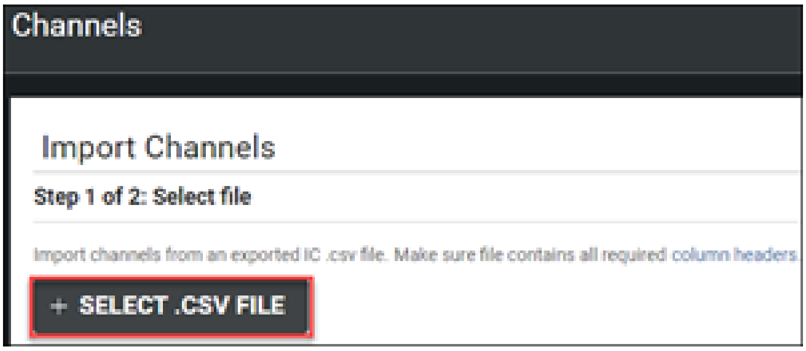
2. Select the '+' (add) button.
3. Select the 'Create assigned channel' button.
4. On the 'Create assigned channel' screen, complete the required and other relevant fields for the new channel. For example:
   - **Spoken Language:** The **Translations** feature uses this to determine what language is heard on this channel.
   - Toggle on **Translation**, **Ops Log**, and/or **Recorded** if using those features for this channel.
   - Add people and groups to the channel.
5. Select the 'Save' button. A message appears indicating the channel was successfully saved. The new channel now appears in the 'Assigned channels' list.

8.2.8 Bulk add multiple channels

> **Note:** Associating people (users) to bulk imported channels must be done manually.

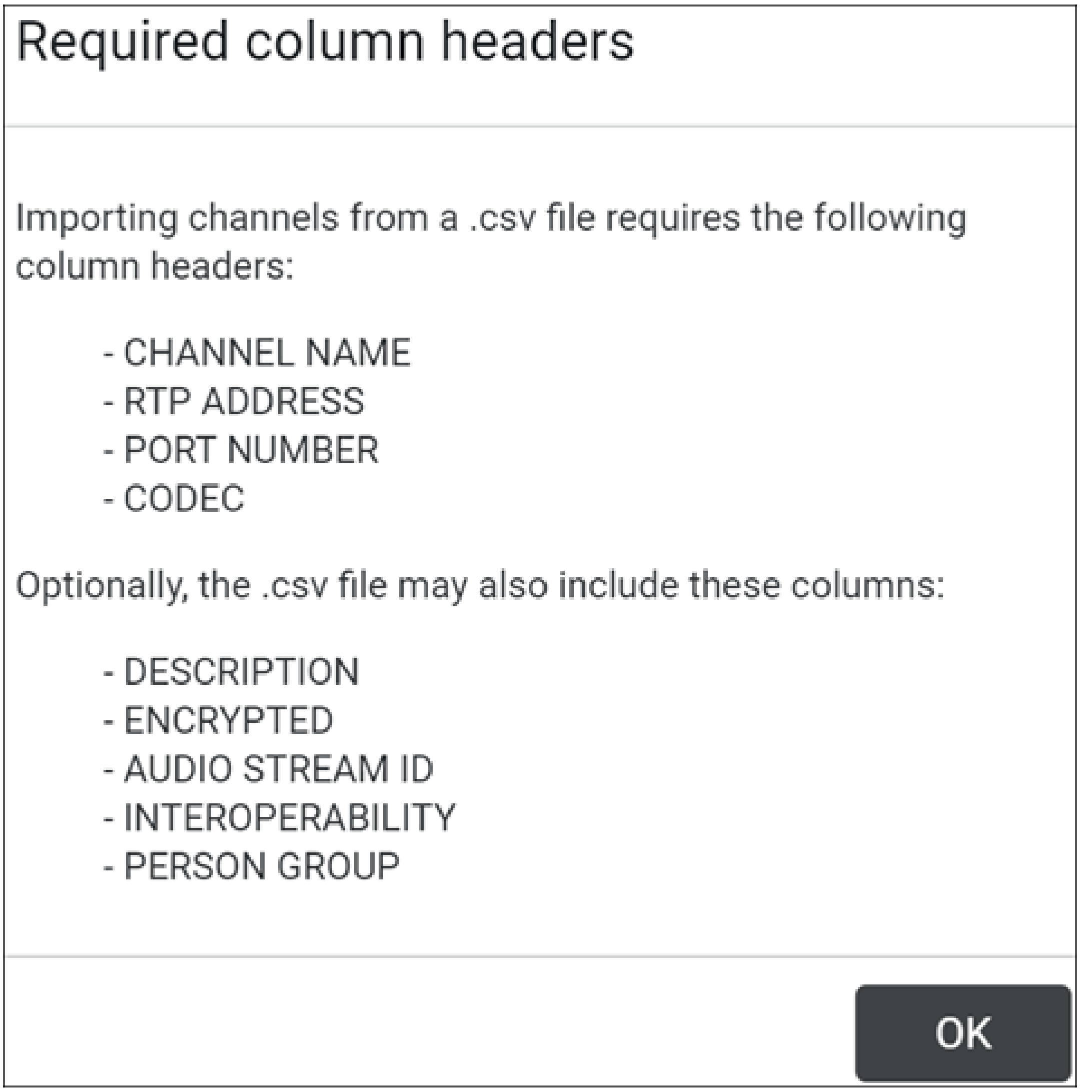
1. Navigate to Settings > Channels.
2. Select the 'Import Channels' button. 

3. From the 'Import channels' screen:



   1. Select a .CSV file to upload.

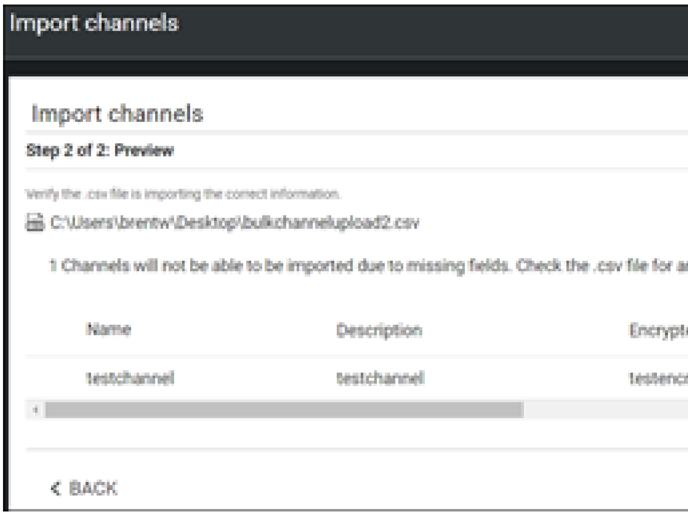
      The file contains the following headers (and corresponding info for each channel being up-loaded):



Here is an example .CSV file:

```
CHANNEL NAME,RTP ADDRESS,PORT NUMBER,CODEC,ENCRYPTED,DESCRIPTION
Fire Dept,239.174.0.1,21000,G.711,Y,Fire Dept
ITService,239.174.0.2,21002,G.711,Y,ITService
Operations,239.174.0.3,21004,G.711,Y,Operations
Help Desk,239.174.0.4,21006,G.711,Y,Help Desk
Technical PMs,239.174.0.5,21008,G.711,Y,TAC
Engineering,239.174.0.6,21010,G.711,Y,Engineering
HRMgmt,239.174.0.7,21012,G.711,Y,HRMgmt
Management,239.174.0.8,21014,G.711,Y,Management
Faculty,239.174.0.9,21016,G.711,Y,Faculty
Students,239.174.0.10,21018,G.711,Y,Students
```

2. Select the ‘Next’ button.

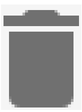


3. Use the data preview to verify the .CSV is correct.
4. Select the 'Import' button. A message appears indicating the channels were imported successfully. All of them now appear in the 'Assigned channels' list.

8.2.9 Edit a channel

1. Navigate to Settings > Channels.
2. Scroll through or search the 'Assigned channels' list.
3. Select the Edit () button for the channel.
4. From the 'Edit assigned channel' screen, update the channel's fields.
5. Select the 'Save' button. A message appears indicating the channel update was successfully saved.

8.2.10 Delete a channel

1. Navigate to Settings > Channels.
2. Scroll through or search the 'Assigned channels' list.
3. Select the  button for the channel.
4. A screen appears asking you to confirm deletion. Select the 'OK' button.
5. A message appears indicating the channel was successfully deleted. The channel no longer appears in the 'Assigned channels' list.

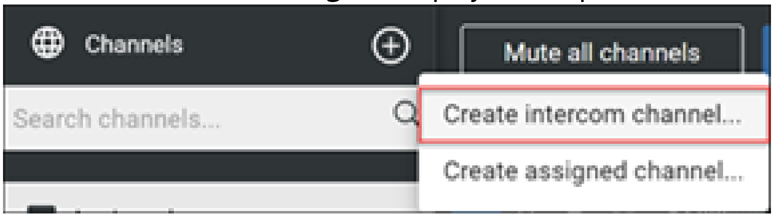
8.2.11 Create Intercom Channel

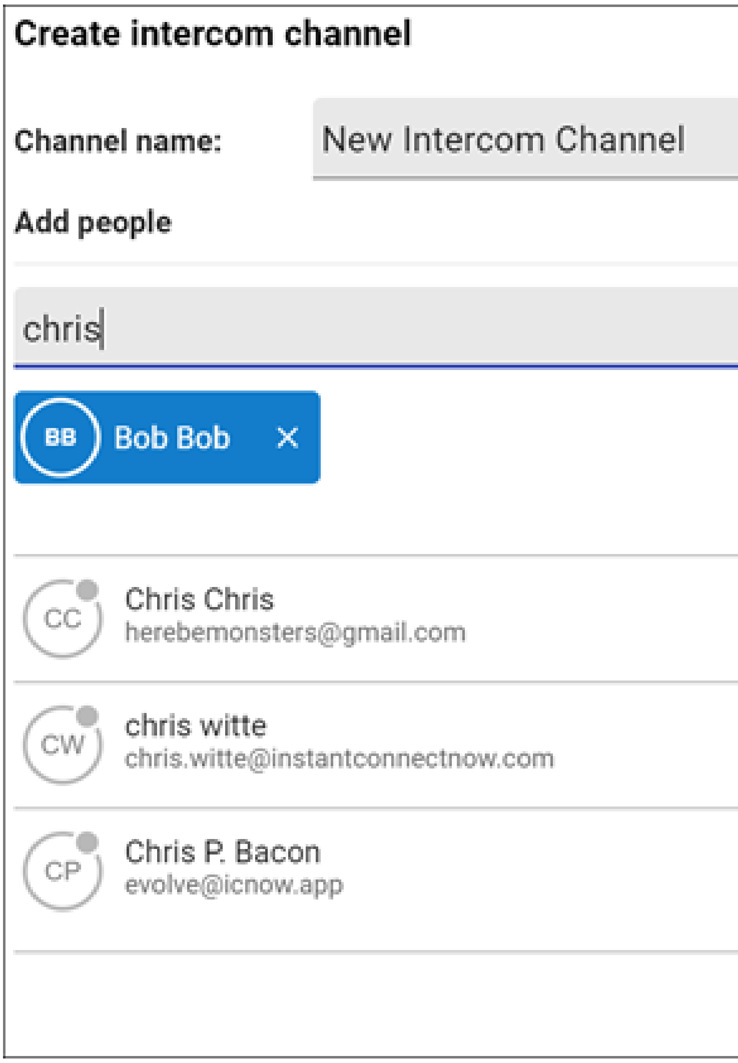
Intercom channels provide the ability for any user to create a channel between them and one or more other colleagues. Intercom channels are created by finding and selecting other users from an user search box.

All settings for the intercom channel are server defined and not visible or editable by the user.

Intercom channel resources are recycled when only one person remains associated with the intercom and the channel is removed from the client dashboard.

To create an intercom channel, follow these steps:

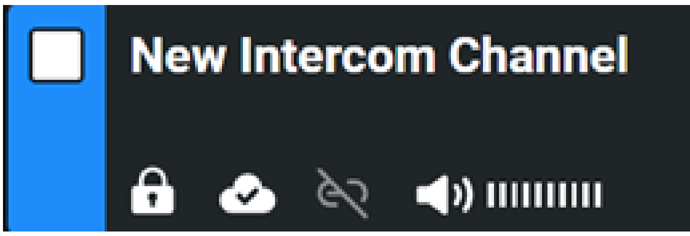
From the Channels list header click the **Plus sign** to display the drop-down menu and select **Create Intercom channel**. 



In the Search field, enter some or all of name of the user.

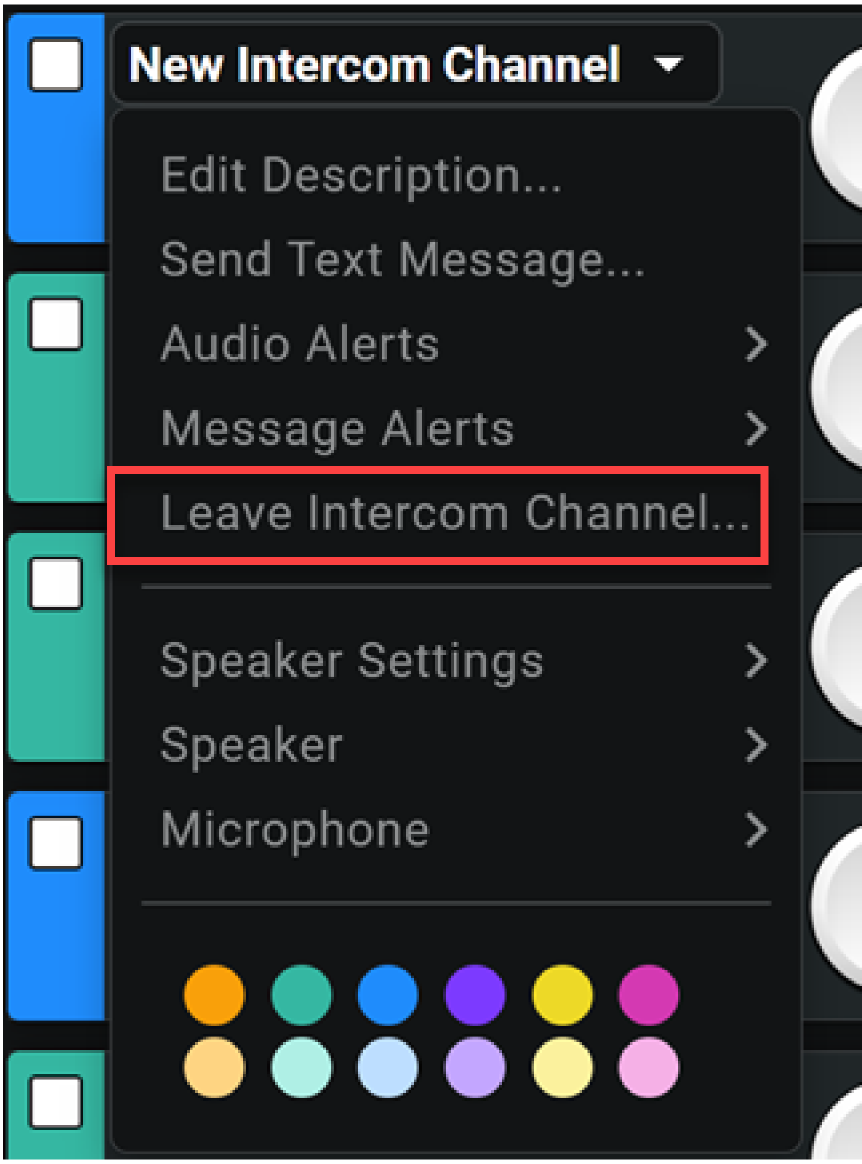
Click the **+** icon for the user to add.

After you add all users, click **Create**



The new Intercom Channel is added to the Channels screen.

To leave an intercom channel: From the channel card dropdown, select 'Leave Intercom Channel',



then select 'OK' on the 'Are you sure?' popup.

8.3 Locations

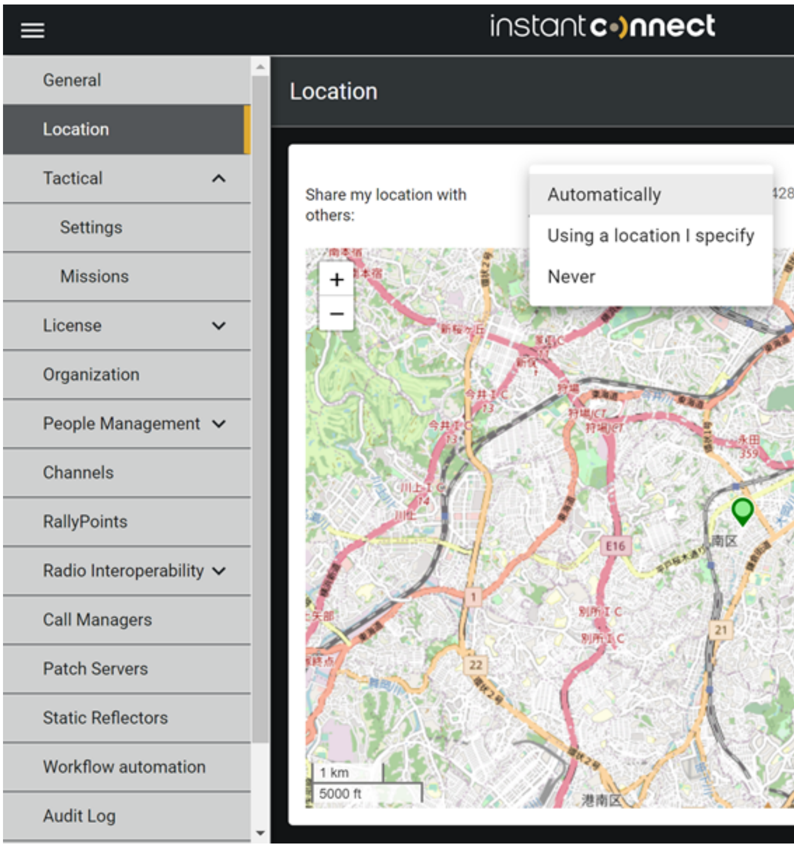
8.3.1 Configuring and Viewing Locations

Instant Connect Enterprise clients have the ability to provide location updates on each device. ICE Desktop clients need to select either a manual location or allow for network based location to share. ICE Mobile client will GPS based location if location sharing is enabled.

8.3.2 Configuring Location Options

Use the Location screen to configure how you provide location information for a ICE Desktop client that you have logged on to. This screen also displays a map that shows your location.

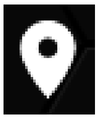
The Location screen is opened from the Location menu option in the Settings window. Click the Settings button to open the Settings window. Select Location from the Settings menu.



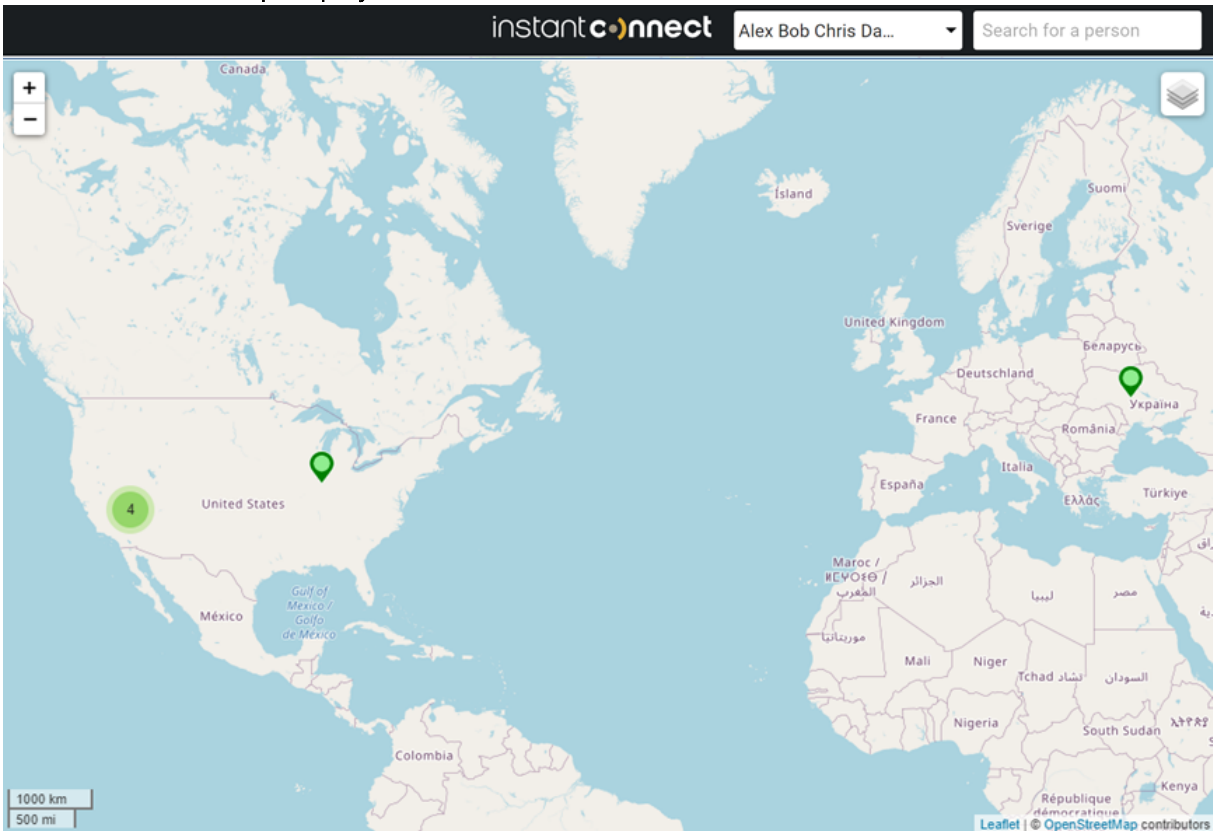
The following figure describes the Location screen.

Setting	Description
Share my location with others	Method that the system uses to share your location. - Automatically - Network based location - Using a location I specify - Manually set location - Never - Does not send location updates
Location coordinates	Location coordinates that you are broadcasting.
Location Pin	Your approximate location, based on your network location capabilities.

8.3.3 Viewing Locations of Members of a Channel

You can view the locations of the device of each active member of a channels, if GPS is enabled on the device. To do so, click the Map icon on the Channels screen. 

Clicking the Map icon opens the Team Locations screen. **All Channels** is selected by default this will display the location for all users logged into the system with at least one channel the same as your user account. To see user locations for a single channel select the channel from the the channel list. The map displays the location of the devices of active users for the selected channel.

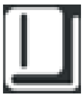
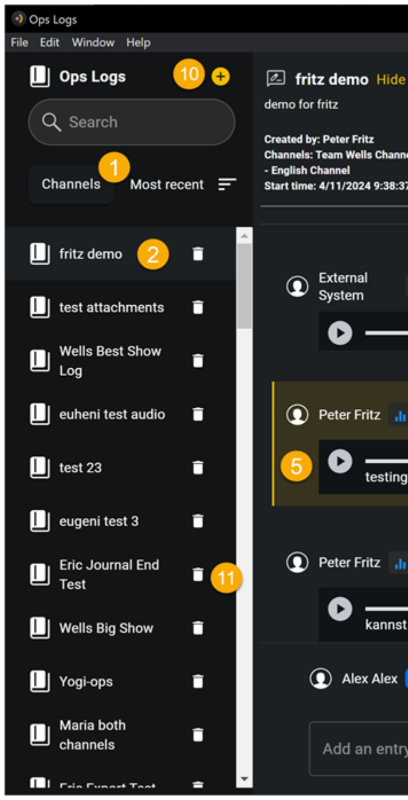


8.4 Ops Log

> **Note**: To access Ops Log you must be an ICE Desktop Admin or an Ops Log Administrator.

Ops logs capture all activity that occurs on specific channels, e.g., transmissions, messages, translations, alerts, etc. These logs can be reviewed, supplemented and commented on. When ended, the entire ops log can be downloaded.

8.4.1 View Ops Log

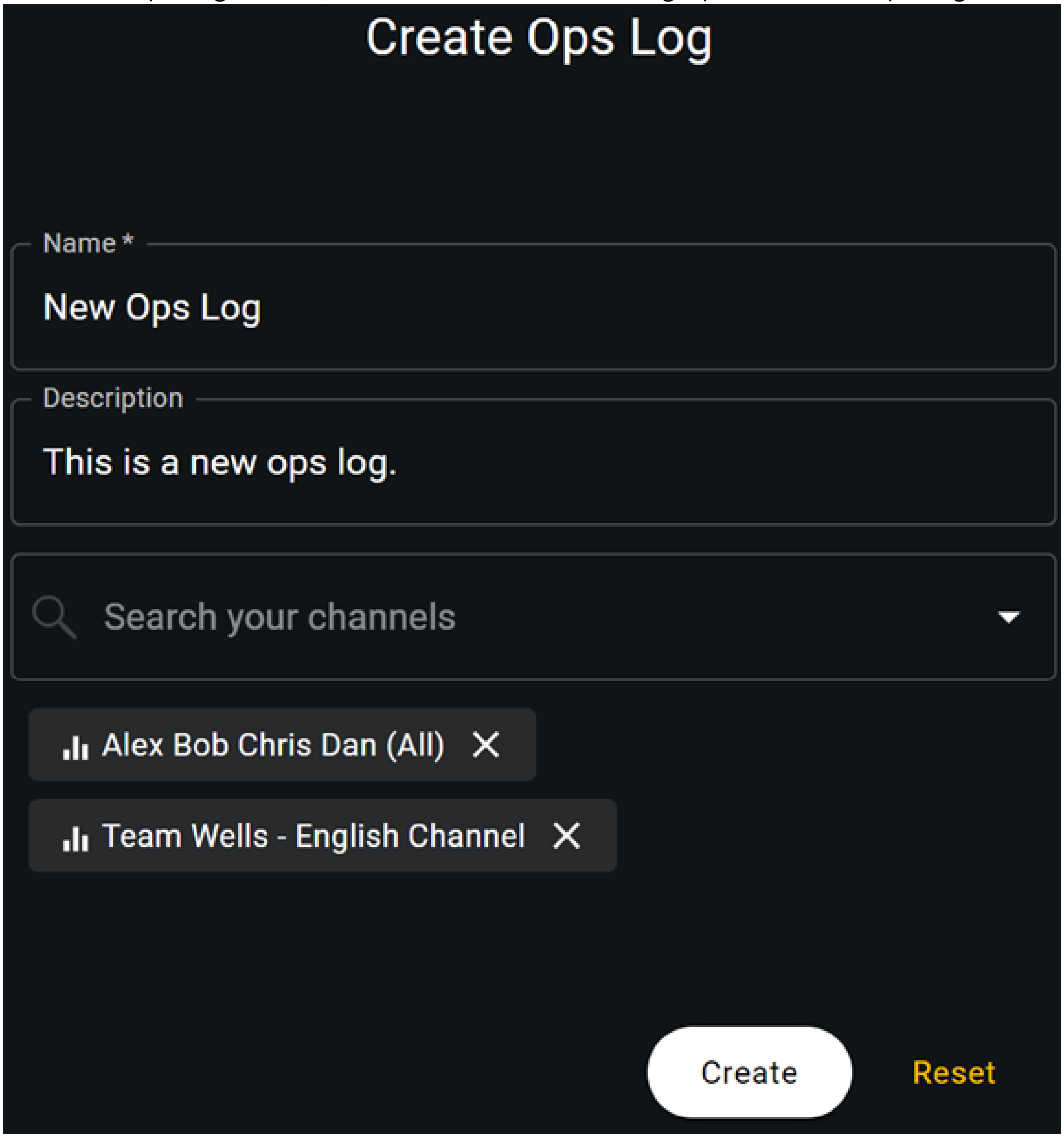
From the dashboard, select the  button to bring up the Ops Log popup screen. 

Features	Description
1	Search by name. Toggle between channels and ops logs. Sort by most recent or alphabetical.
2	Select an ops log to view.
3	Review all of the entries in the selected ops log.
4	Select a channel and add an entry to the ops log. Entries can be text or a file attachment (e.g., image, audio).
5	Select an entry in order to review comments. Comments are clarify or add more info to the entry.
6	Review the comments on an entry.
7	Add a comment to an entry.
8	Select 'End' to stop the ops log. Once the ops log is ended, no further entries or comments are recorded.

Features	Description
9	Once the ops log is ended, it can be downloaded. Downloads include all entries, comments, attachments, etc.
10	See the ‘Create an ops log’ section below.
11	Delete an ops log.

8.4.2 Creating an Ops Log

1. From the 'Ops Log' screen, select the + button to bring up the 'Create Ops Log' screen.



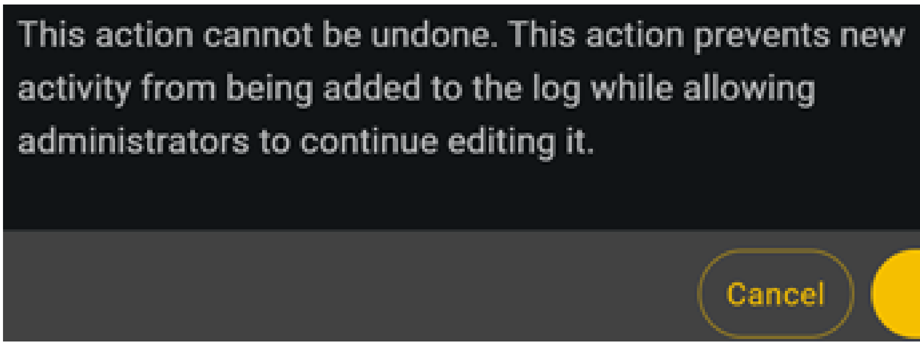
2. Name the ops log.
3. Select the channel(s) for the ops log.

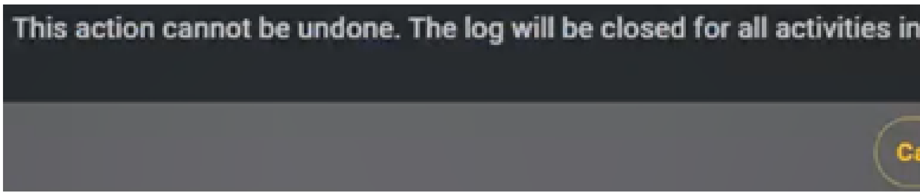
> **Note:**
>
> - Both the 'Ops Log' and 'Recorded' features must be enabled on the channel(s) or they will not be available for inclusion in an ops log.

> - Ops Log Admins will only see channels to which they belong.

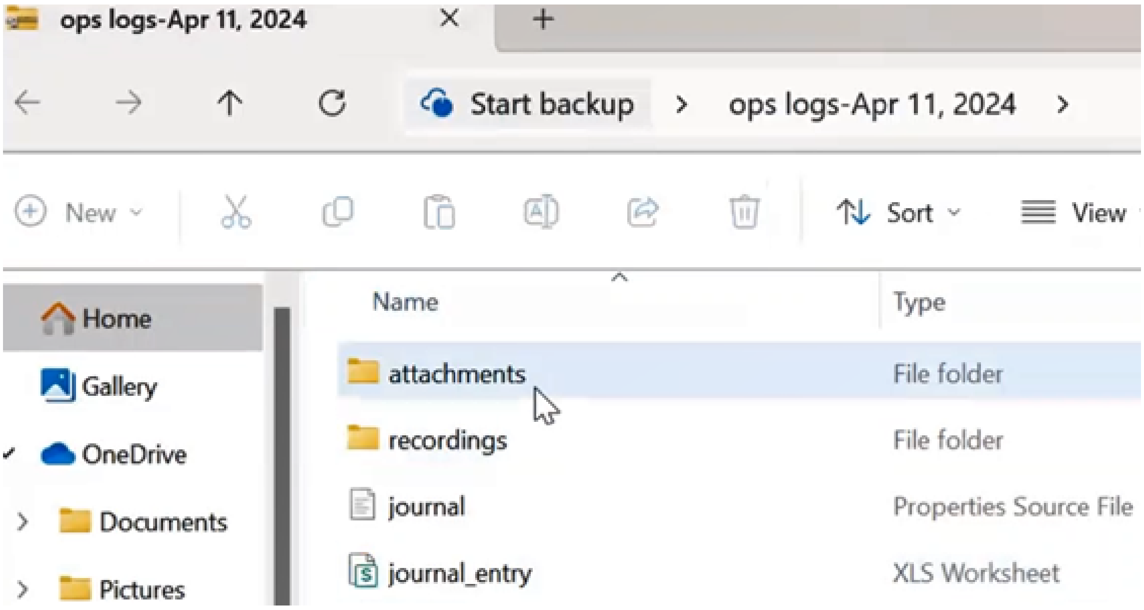
4. Select 'Create'. The new ops log now appears in the ops log list.

8.4.3 Download an ops log

1. Select an ops log.
2. Select 'End' to stop the ops log.
3. Select 'OK' on the warning screen. 

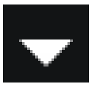
4. A banner displays confirming the ops log is ended.
5. The 'End' button now becomes the 'Archive' button. Select 'Archive' button.
6. Select 'OK' on the warning screen. 

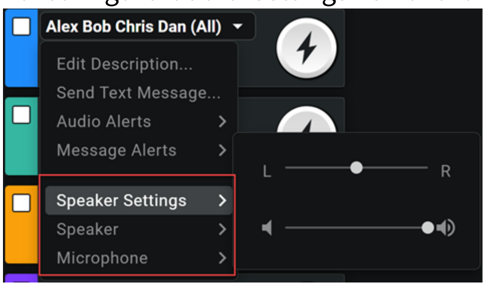
7. A banner displays confirming the ops log is archived.
8. Now the 'Download' button is activated, so select it.
9. Select the download location for the ops log archive.
10. The ops log archive is a .zip folder containing all attachments, recordings, entries, and com-



ments.

8.5 Channel Audio Settings

To configure audio settings for a channel, select the  dropdown from the channel card.

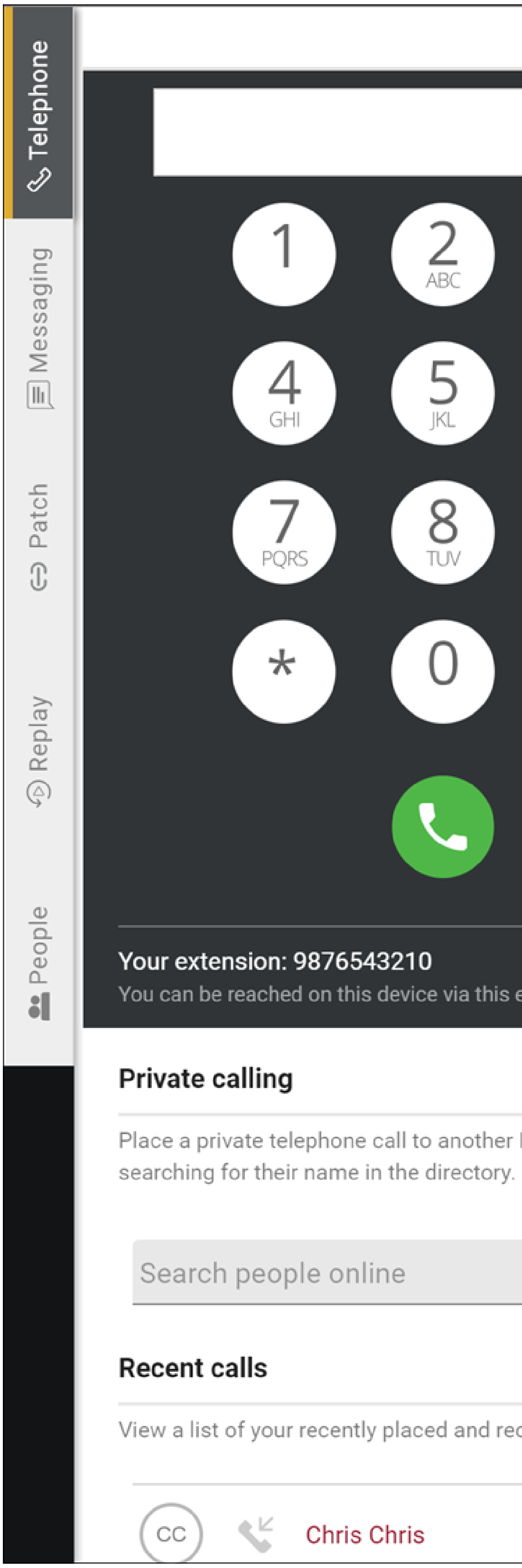


- **Speaker Settings**: Set the balance between right and left speakers, and set overall channel volume.
- **Speaker**: Select the speaker that plays audio from the channel.
- **Microphone**: Select the microphone to use for this channel.

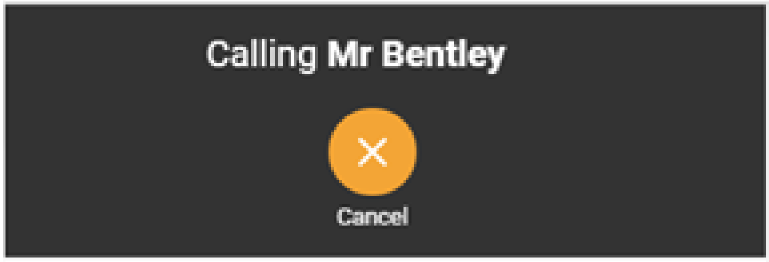
8.6 Telephone

ICE Clients have the ability to make and receive telephone calls within the application. These calls are connected via the IP network and do not utilize the cellular phone plan.

To make and receive phone calls your system administrator will need to configure your user account with a phone number.



Making a call - Click on the Telephone tab to open the Telephone panel.

From the telephone panel you can make a call by dialing a phone number with the dial pad and click on the green call icon. The call will be sent to the phone number. The call progress screen will be displayed with an audible ring back. 

Press the Cancel button to hang up the call.

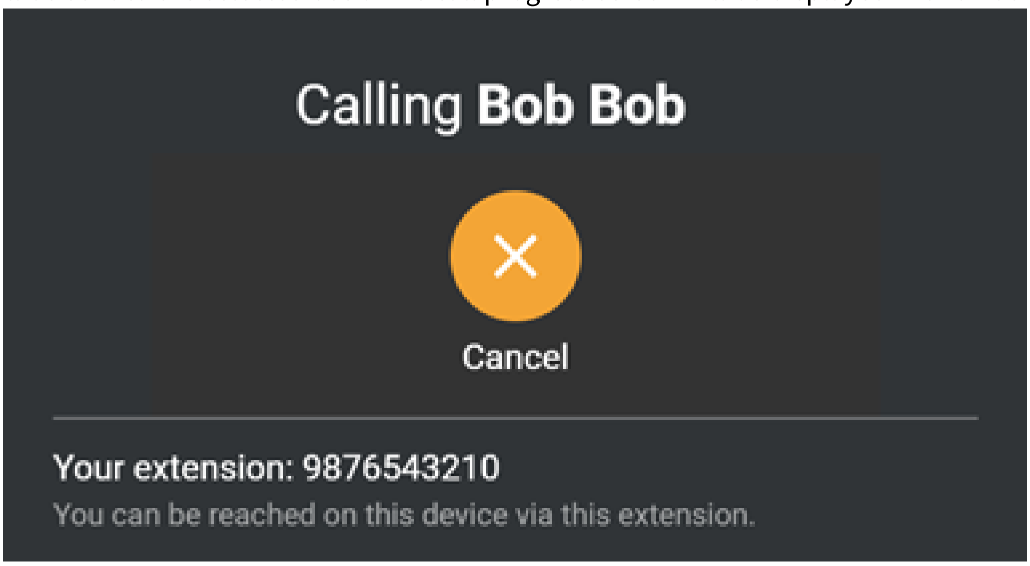
8.6.1 Making a Private Call

The Private Call feature provides the ability for the user to Make, Receive private full-duplex calls from the ICE Desktop client to another ICE client.

Start typing the name of the user in the Search Users search box 

A filtered list of users will be displayed. Users that are online will be displayed with a green call button, offline users will be displayed with a gray call button.

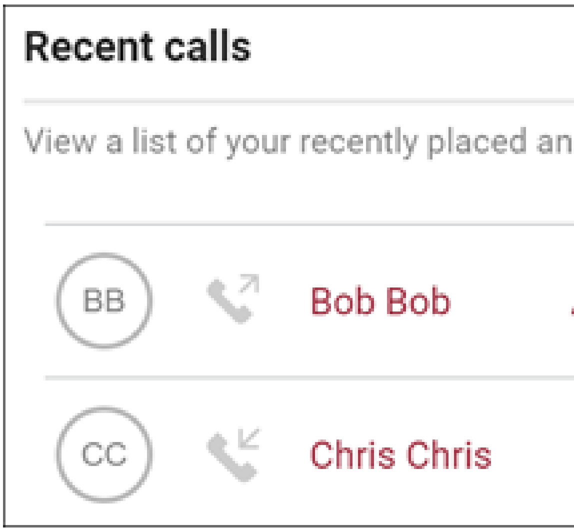
Select the user to call from the list and tap on the green call button.

The call will be sent to the selected user. The call progress screen will be displayed with an audible ring back. 

Press the Cancel button to hang up the call.

8.6.2 Recent Calls

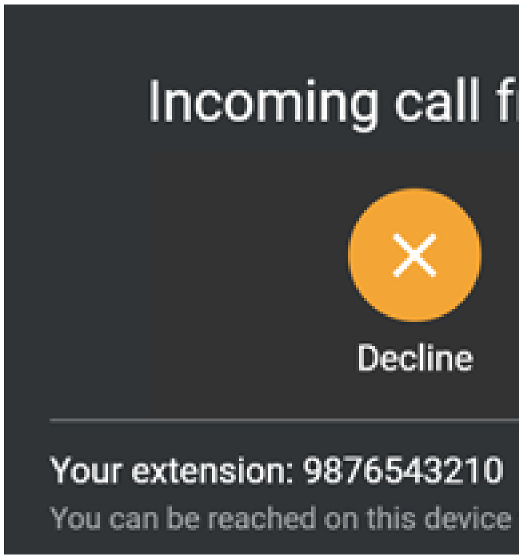
The Recent Calls list provides the user a historical list of call activity. From the recent call list the user has the ability to place a call to the user or number listed in the record.



To place a call from the Recent Call list find the user / number you want to call and click on the green call button.

8.6.3 Incoming Call

The Incoming call notification allows the user to decline or answer the call.



Tap the Decline button to reject the call and continue to use the application without an active call.

Tap the Accept button to answer the call and talk with the caller.

8.6.4 Active Call

The active call screen provides the user in call controls.

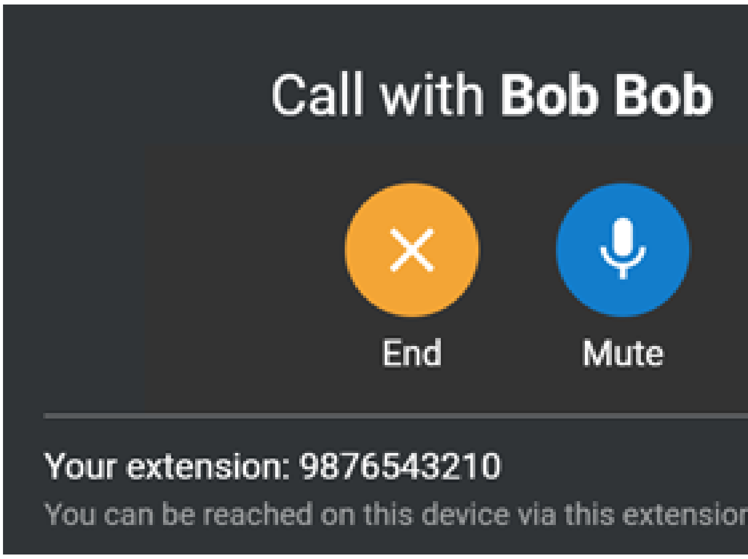
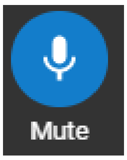
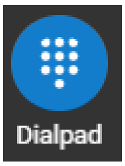


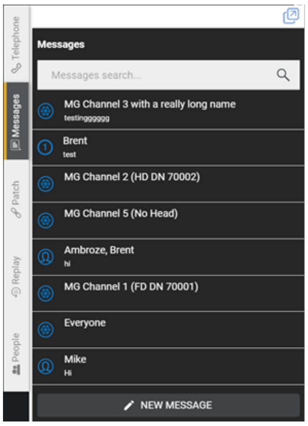
Table 8: Active Call Buttons

Icon	Description
	End / Hang-up the call
	Mute / Unmute the mic on the call
	Displays the dial pad to allow the user to send DTMF tones in the call

8.7 Messaging

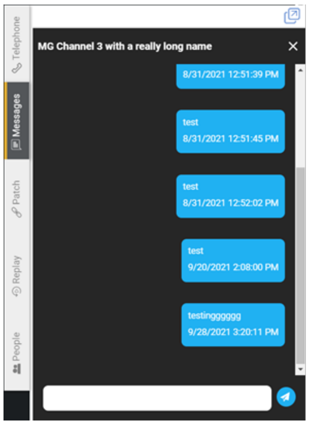
The Messaging tab is where users can send and receive instant messages via conversations, which are chat groups based on either a channel or a selected group of users.

- Displays a list of recent and ongoing conversations
- Allows searching for conversations by channel or people names.



8.7.1 View or send a message

1. Search for and select the relevant conversation.
2. View the conversation thread or enter a new message and send it.



8.7.2 Start a new conversation

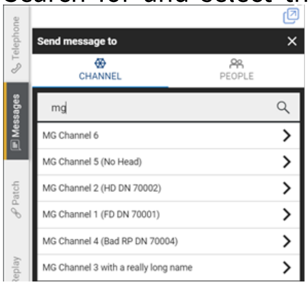
1. Select the **Messaging** tab.
2. Select the **New Message** button.
3. Select either **Channel** or **People**.
   - Channel: The conversation participants consist of the members of a channel.

    - People: The conversation participants consist of one or more people, regardless of their channel associations.

4. Create the conversation.

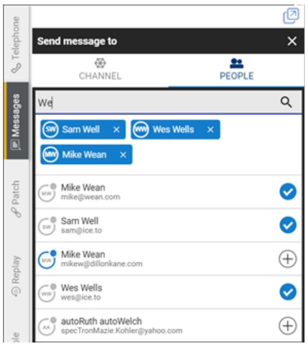
For Channel:

1. Search for and select the channel. You must be associated with the channel to select it.



2. The conversation is created and messages can be sent.

For People:



1. Search for and select one or more people (via the **+** button).
2. Select the **New Message** button.
3. The conversation is created and messages can be sent.

8.7.3 Edit or delete a message

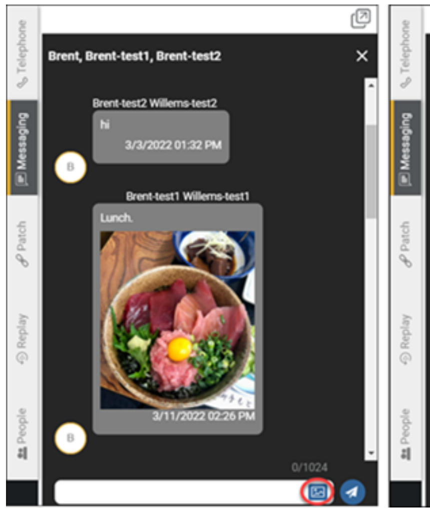
1. Right-click on the message.
2. Select either **Delete message** (to delete it) or **Edit message** (to edit it). If editing:
    1. The message populates the message text box and can be edited.
    2. When done editing the message, send it.
    3. The edited message overwrites the original message in the conversation.

8.7.4 Share an image/video via messaging

8.7.4.1 Supported file types Natively supported file types display as a thumbnail. Unsupported file types display with a placeholder icon.

- Image
  - .gif
  - .jpg .jpeg .jfif .pjpeg .pjp
  - .png
  - .svg
- Video
  - .mp4

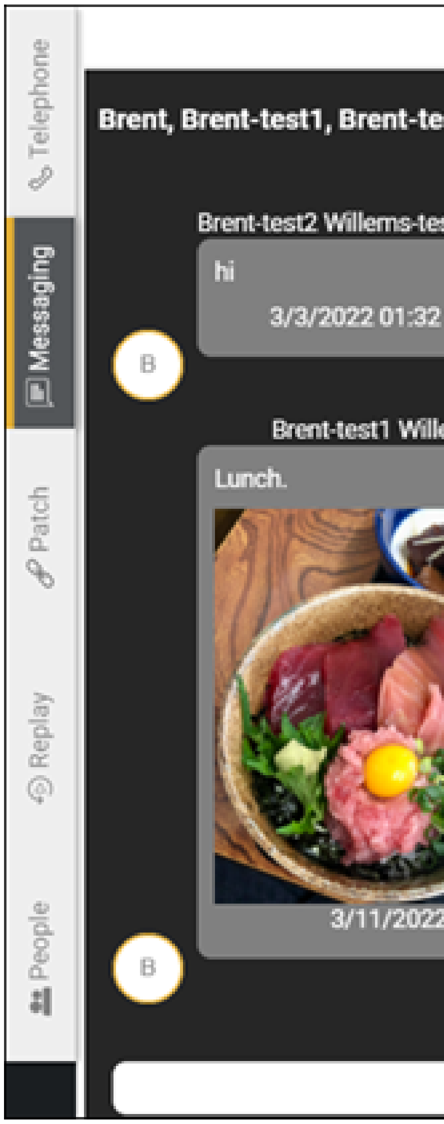
To share an image/video



1. From the relevant conversation, select the image/video attachment button.
2. From the resulting File Explorer (Windows) or Finder (MacOS) interface, select the existing image/video.
3. Once the image/video is attached to the message, send it.

> **Note:** Image and video files are deleted after 14 days (default timeframe, this is configurable). Users will see a “This file is no longer available” message in their message history.

To view or save an image/video



1. From the relevant conversation, right-click on the image/video thumbnail.
2. Select 'Open' to open the file in the OS's native image display or video player function.

   OR

   Select 'Save' to save the file locally via the File Explorer (Windows) or Finder (MacOS) interface.

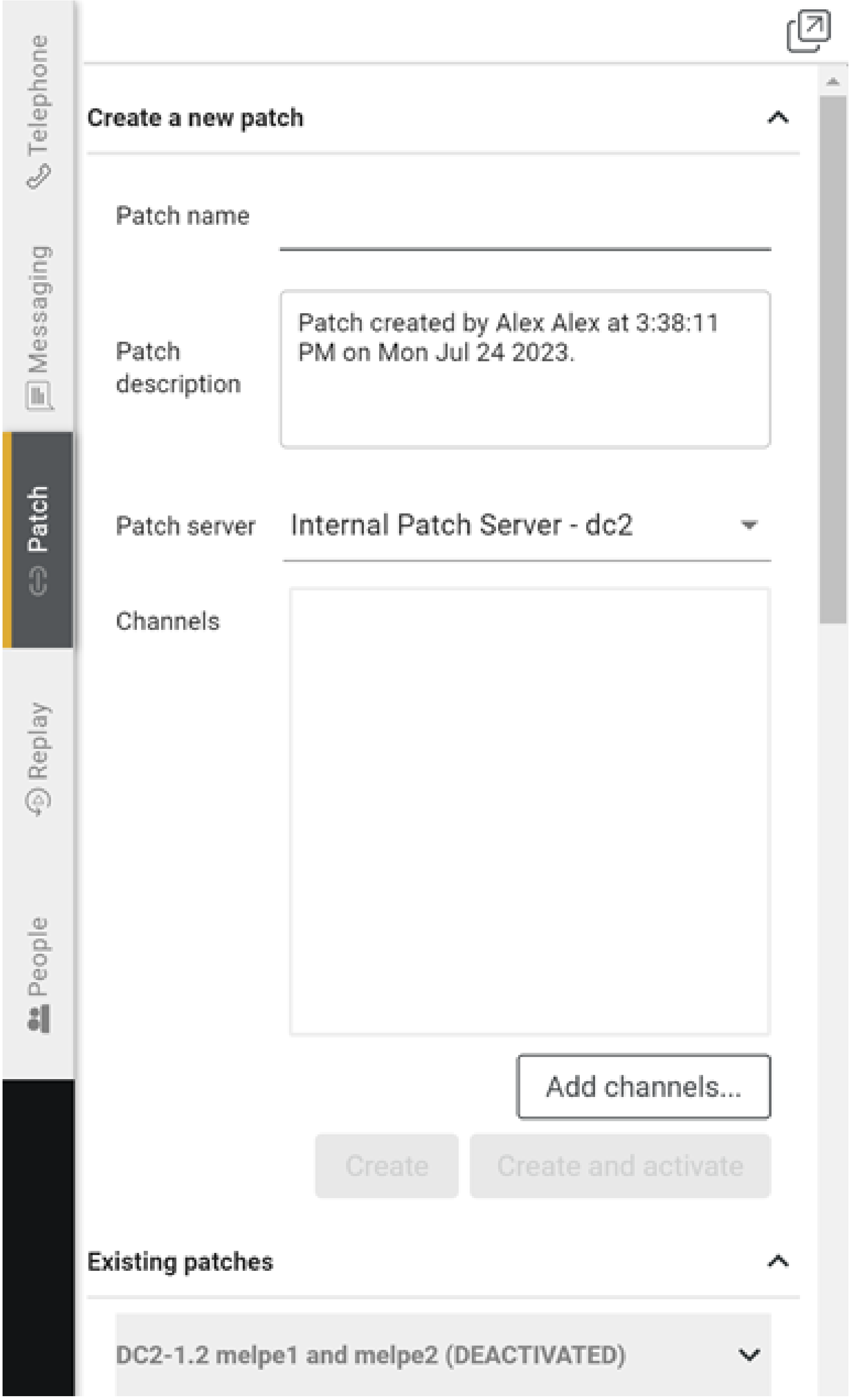
8.8 Patching

Patching is one of several terms used to define the connection of a Instant Connect channel to another channel or channels, resulting in the ability to establish interoperable communications between channels and systems not compatible with each other directly. Some of the other terms used to define this process include "cross-connect", "interconnect", or "bridging". Patching can be initiated by a user granted the Patch Agent privilege using the Patch tab on the Instant Connect Desktop.

To manage patches on Instant Connect Desktop, select the **Patch** tab.

> **Note:** You also can select 'Create Patch' from a channel card options dropdown menu in order to access the 'Patch' tab.

If the **Patch** tab is not available check with your system administrator to verify that your user account has been provisioned with the Patch Agent privilege.


Telephone
Messaging
Patch
Replay
People
Create a new patch
Patch name
Patch description
Patch created by Alex Alex at 3:38:11 PM on Mon Jul 24 2023.
Patch server
Internal Patch Server - dc2
Channels
Add channels...
Create
Create and activate
Existing patches
DC2-1.2 melpe1 and melpe2 (DEACTIVATED)

The **Patch** tab allows the user to Create, Delete, Activate and Deactivate channel patches, assign a patch to a specific Patch Agent and view the status of exiting patches running on the Instant Connect system.

8.8.1 Create Patch

> **Notes:**
>
> - Do *not* create patches with multicast channels.
> - Only enterprise channels can be patched. Mission channels can *not* be patched.

Use the **Create a new patch** form on the Patch tab to enter the information and channels for your new patch.

- **Patch Name**: Name of the patch. If left blank the default name will be the channel names.

- **Patch Description**: Description of the patch. Default: Patch created by <user name> at <time / date>

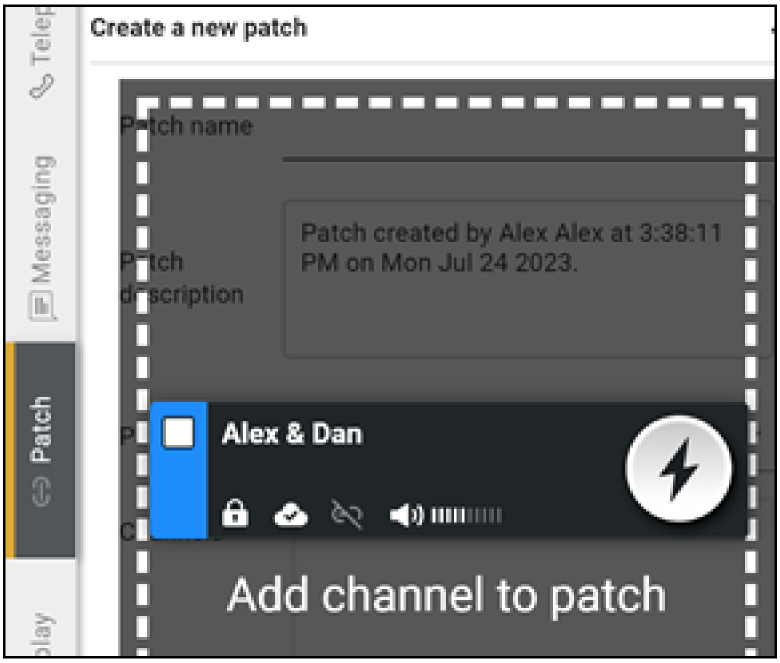
- **Patch Server**: List of available patch servers on the system.

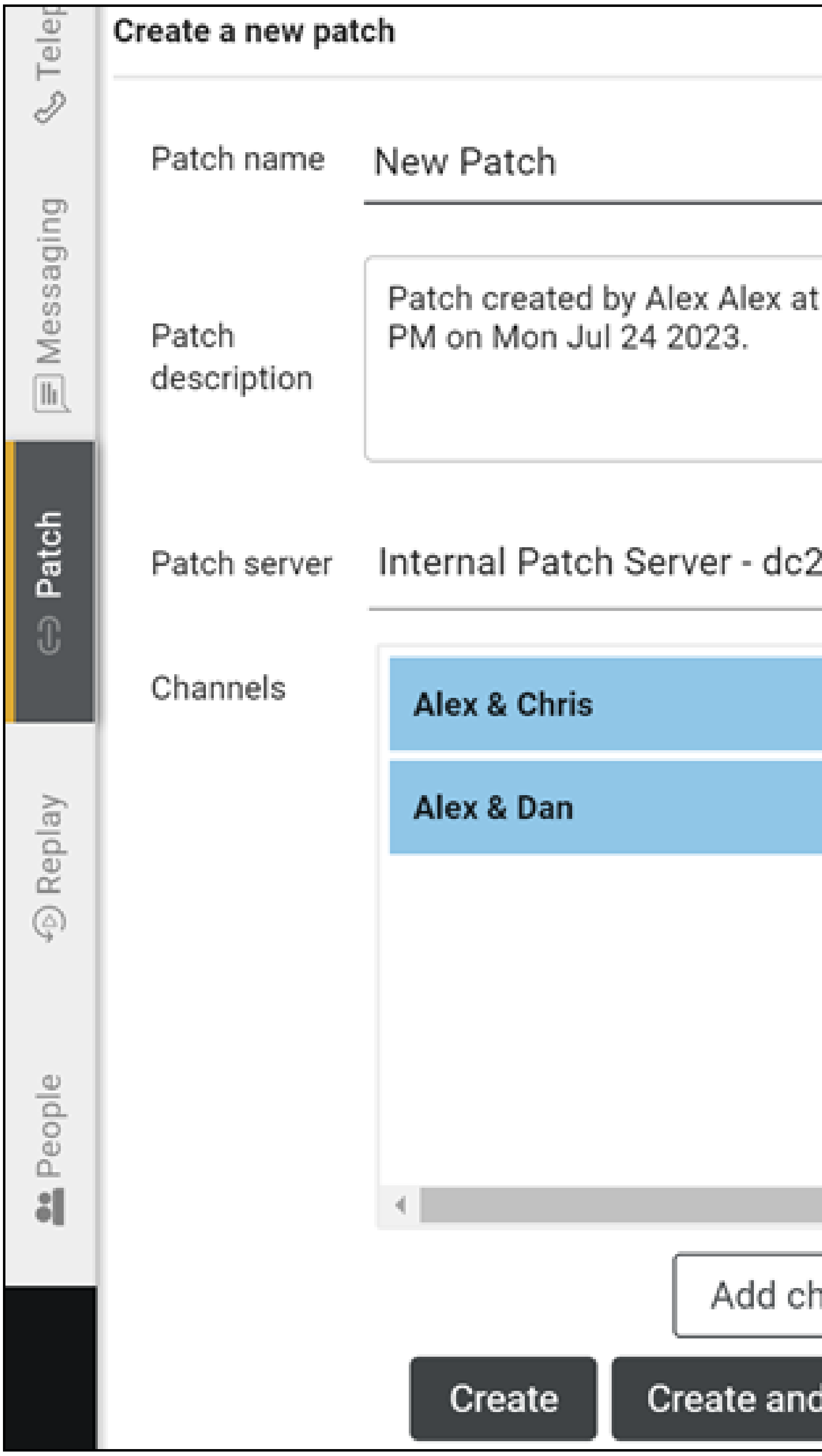
- **Channels**: Drag and Drop channel cards in to the box to add them to the patch

- **Create**: Create button will save the patch configuration into the list of existing patches without Activating the patch.

- **Create and activate**: Create and activate button will save the patch configuration into the list of existing patches and activate the patch on the patch server

Enter the name of you patch in the **Patch name** field, enter a **Patch Description**.

Drag and drop channels in to the **Channels** box: 



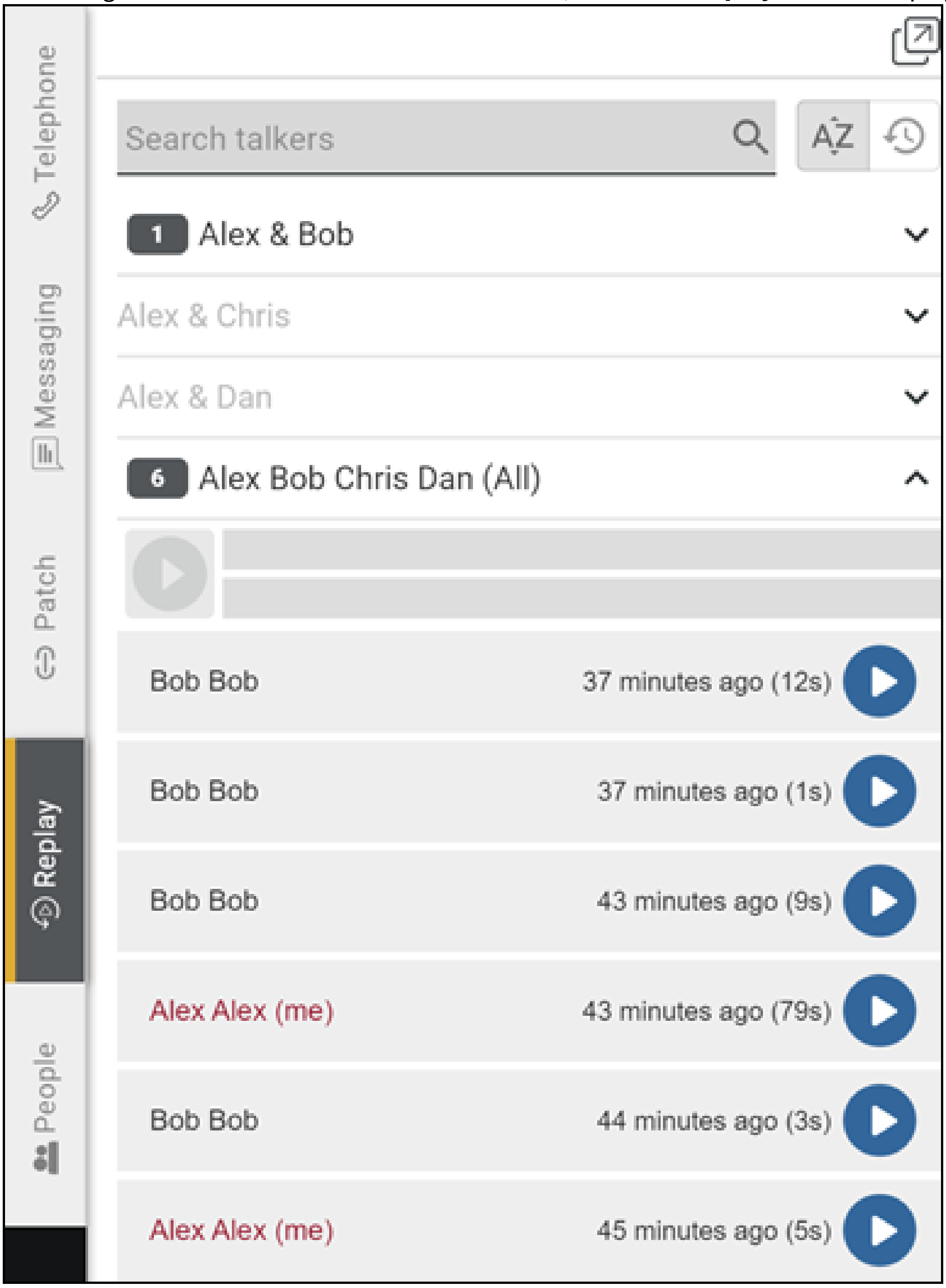
Click the **Create** or **Create and activate** button.

The patch will be displayed in the list of existing patches.

If the patch is not already active click on the **Activate** button.

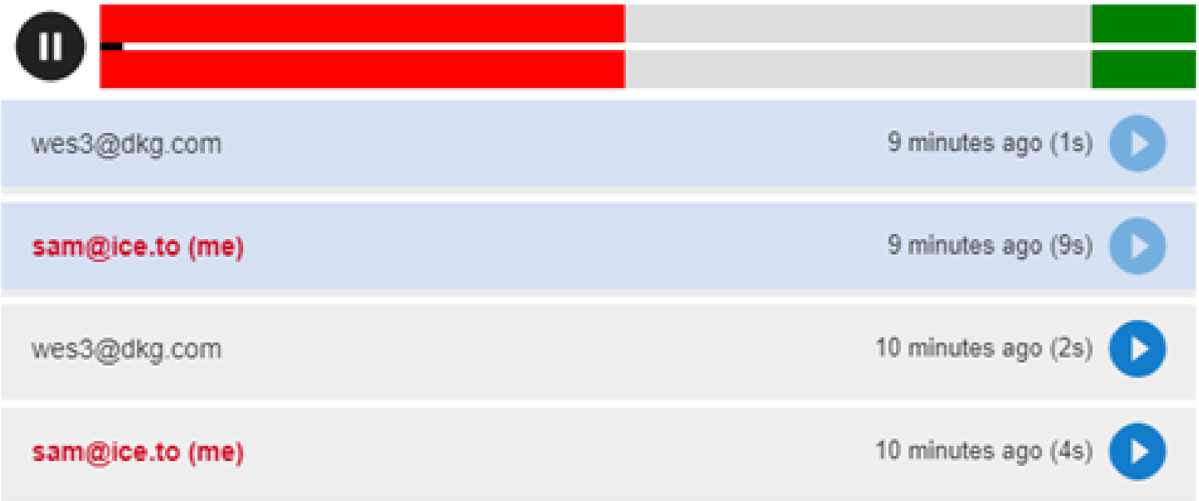
8.9 Replay

To play recordings of audio communication for a channel, select the **Replay** tab. The replay panel opens.



The replay panel displays a list of active channels in use by the user with recorded audio clips available for playback. A clip is a recording of outgoing or incoming audio transmissions from your ICE Desktop for a channel. Your outgoing transmissions are displayed in red type. Incoming transmissions received from other users are displayed in black type.

To play an individual clip, click the Play button that appears to the right of the clip name. Audio clips are displayed from the newest transmitted or received at the top of the list to oldest at the bottom. To play multiple clips, select the oldest audio clip that you want to replay, all newer audio clips will be selected for replay, click the Play button in the top bar. All audio clips will be replayed from the oldest to

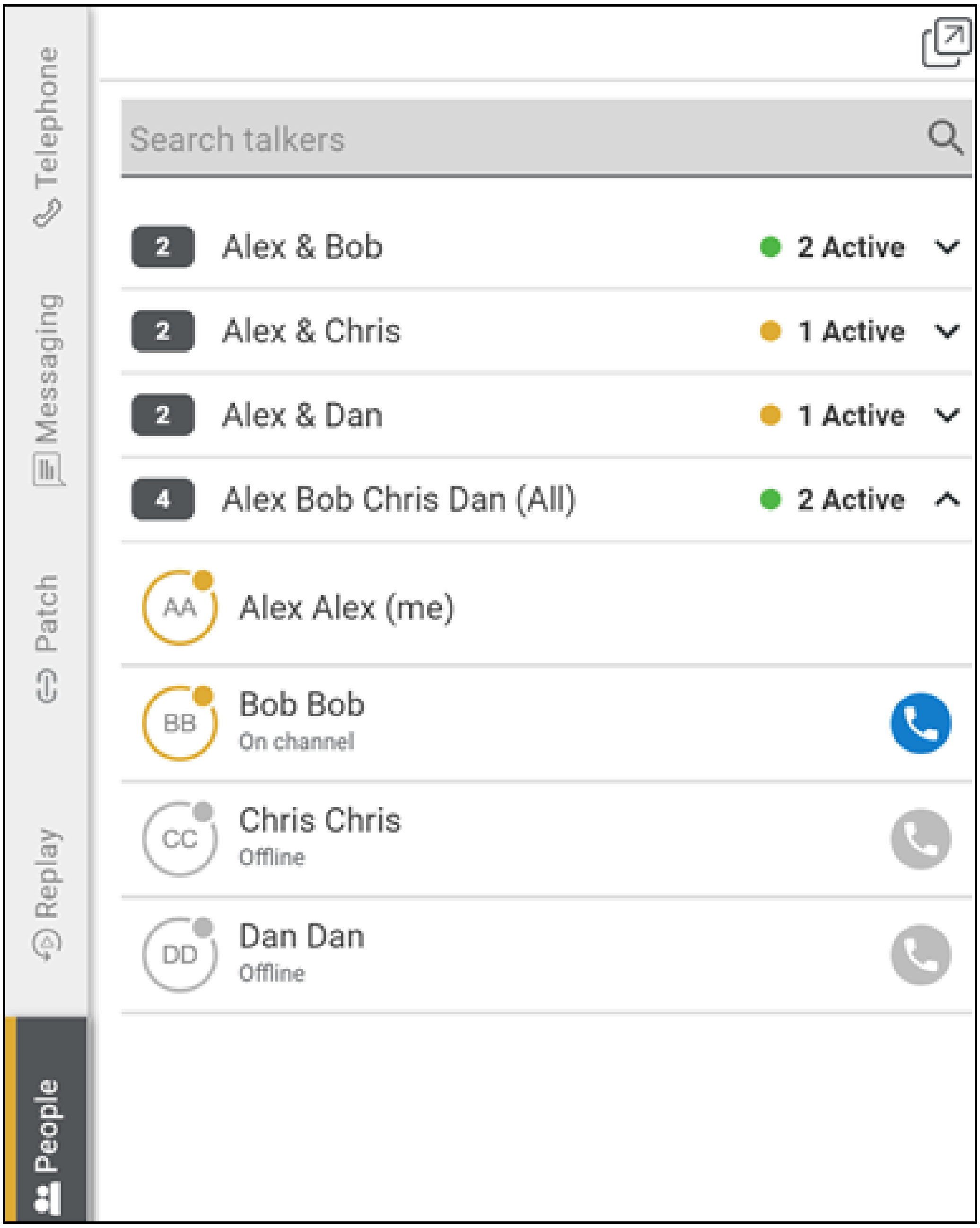


newest.

8.10 People Management

8.10.1 View People

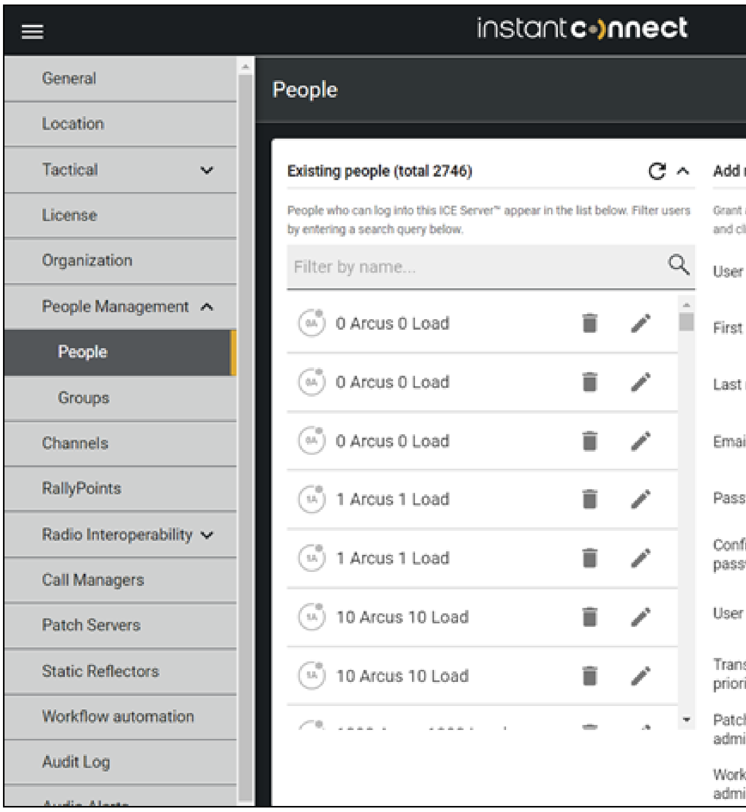
- From the desktop, select the 'People' tab to open the 'People' panel, which displays a list of your active channels including a list of all users provisioned to use each of those channels.



- The panel also provides a 'Search channel or talker' box that filters the channel list per the search string entered.
- Only 20 users can display at a time, please use the search function to find users not displayed.
- The status of each user is displayed with the icon next to their name, the color indicates if they are online (gold) or offline (grey).

8.10.2 View a person

1. Navigate to Settings > People Management > People.



2. Scroll through or search the 'Existing people' list.

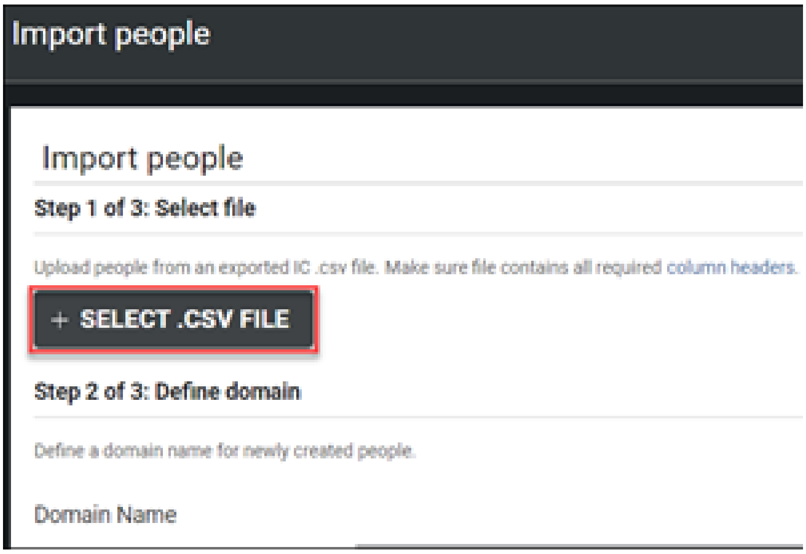
8.10.3 Add a person

1. Navigate to Settings > People Management > People.
2. On the 'Add new person' panel, complete the required fields for the new person.
3. Assign the new person any relevant roles, e.g., patch admin, ops log admin, enable telephony, etc.
4. Assign the new person to any relevant channels and groups.
5. Select the 'Add' button. A message appears indicating the person was successfully added. The new person now appears in the 'Existing people' list.

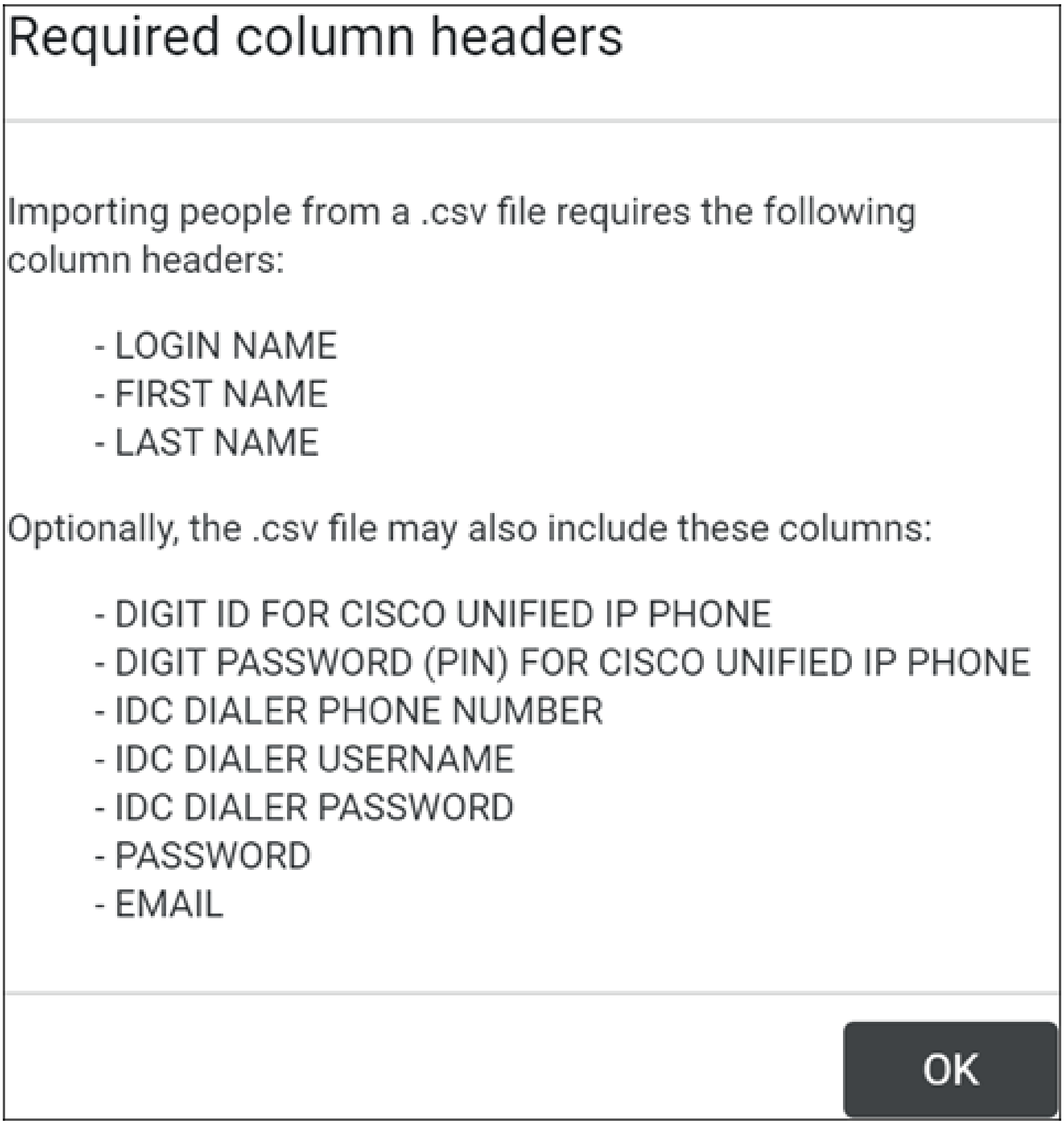
8.10.4 Bulk add multiple persons

> **Note:** Bulk adding (importing) multiple people will not work if LDAP is configured for your domain users.

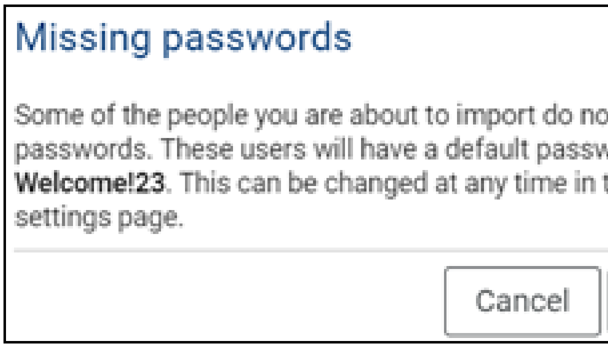
1. Navigate to Settings > People Management > People.
2. Select the 'Import People' button.
3. From the 'Import people' screen:

    1. Select a .CSV file to upload. 

The file contains the following headers (and corresponding info for each person being up-loaded):



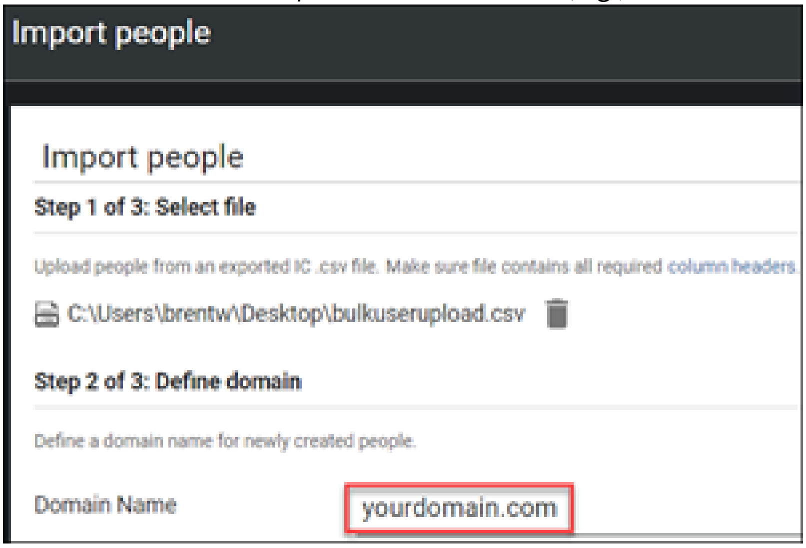
> **Note:** If password is left blank, a default value is assigned:



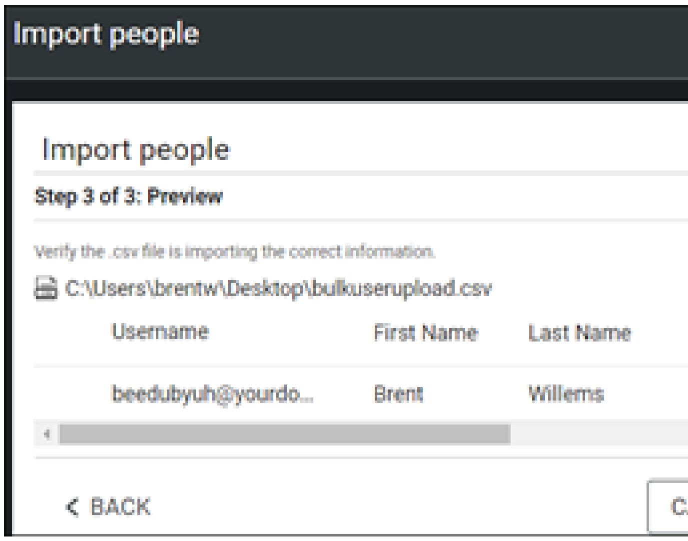
Here is an example .CSV file:

```
LOGIN NAME,FIRST NAME,LAST NAME,PASSWORD,DigitID FOR CISCO UNIFIED
    IP PHONE,DIGIT PASSWORD (PIN) FOR CISCO UNIFIED IP PHONE,DialIn
qatest1,qatest1,Desktop,Welcome123,1001,1001,1001
   qatest2,qatest2,iPhone,Welcome123,1002,1002,1002
   qatest3,qatest3,xcover,Welcome123,1003,1003,1003
   qatest4,qatest4,ecom,Welcome123,1004,1004,1004
   qatest5,qatest5,Mac,Welcome123,1005,1005,1005
```

2. Enter the domain name that will be used in combination with the LOGIN NAME value to create each persons user name (e.g., `LOGINNAME@yourdomain.com`).



3. Select the 'Next' button.



4. Use the data preview to verify the .CSV is correct.

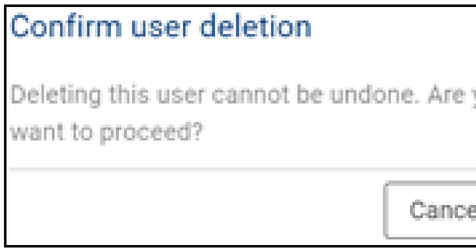
4. Select the 'Import' button. A message appears indicating the people were imported success-

fully. All of them now appear in the 'Existing people' list.

8.10.5 Update a person

1. Navigate to Settings > People Management > People.
2. Scroll through or search the 'Existing people' list.
3. Select the 'Update' button for the person. The 'Add new person' panel becomes the 'Update person' panel and displays the selected person's information.
4. Update the person's fields.
5. Select the 'Update' button. A message appears indicating the person was successfully updated. The 'Update person' panel returns to being the blank 'Add new person panel'.

8.10.6 Delete a person

1. Navigate to Settings > People Management > People.
2. Scroll through or search the 'Existing people' list.
3. Select the 'Delete' button for the person.
4. A screen appears asking you to confirm deletion. Select the 'OK' button. 

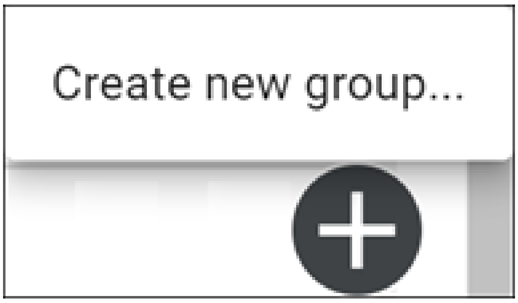
5. A message appears indicating the person was successfully deleted. The person no longer appears in the 'Existing people' list.

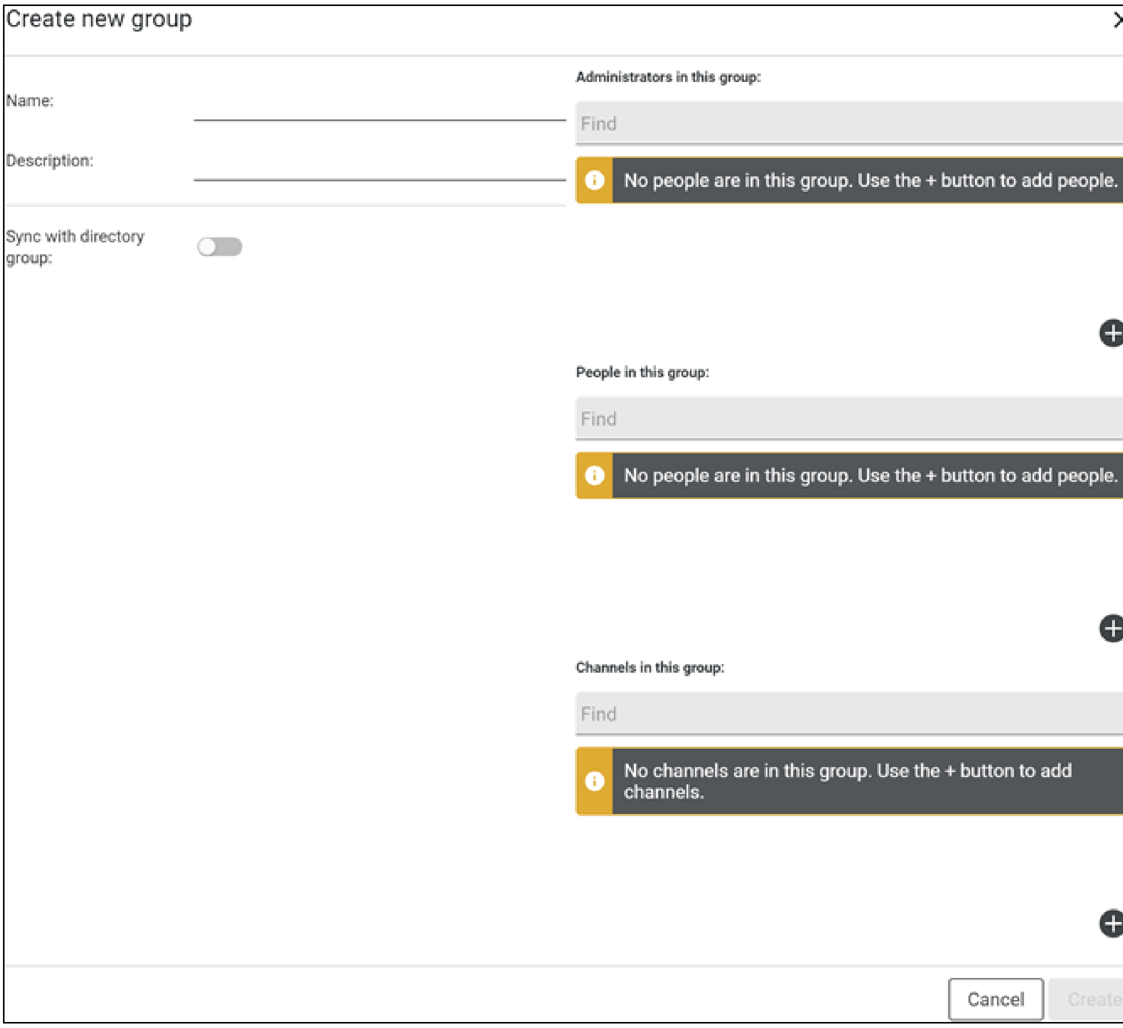
8.10.7 Groups

Organizing people into relevant groups supports quick, targeted communication. The 'Groups' screen allows for the the management (i.e., create, edit, delete) of groups of people.

To Create a group

1. Navigate to Settings > User Management > Groups.

2. Select the ‘Create new group’ button. 

3. Name the group. 

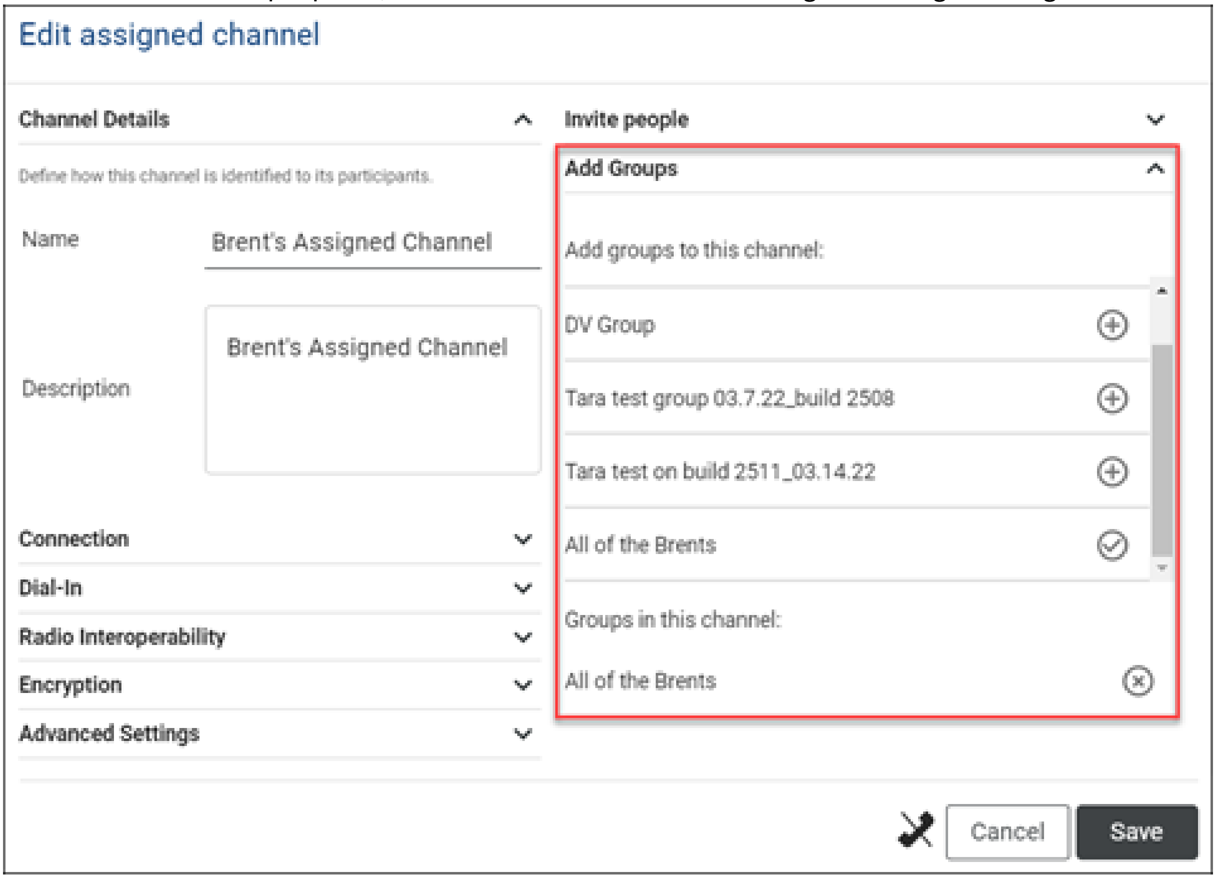
4. Add one or more Group Admins to the group.

> **Note:** Group Admins are not automatically made group members, so if the Group Admin is also to be a group member, then add that person as a member, too. The Group Admin role allows a group member to edit the group’s metadata:
>
> - Group name

> - Group description
> - Group membership (add/remove)
> - Group channels (add/remove)

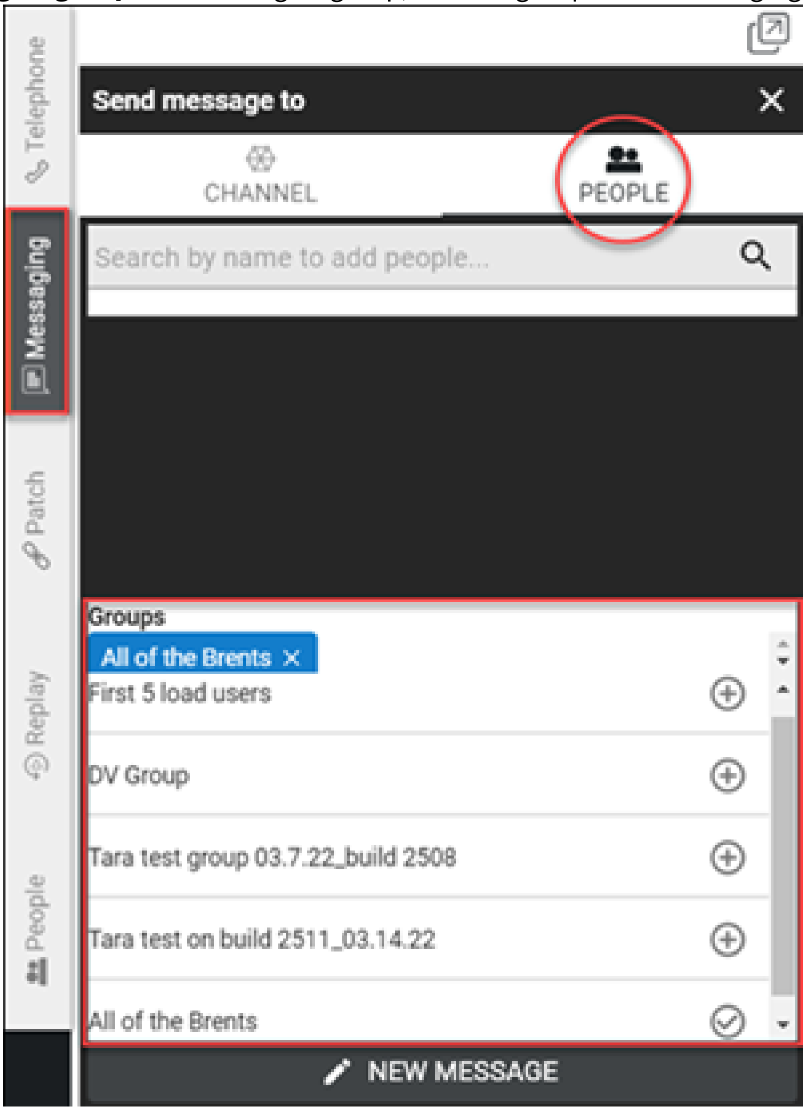
5. Add the rest of the people to the group.
6. Add the relevant channels to the group.
7. Select the 'Create' button. A banner appears: 

8.10.7.1 Add or remove a group to a channel Add or remove a group to an assigned channel via the 'Add Groups' panel, which is accessible when creating or editing an assigned channel.



8.10.7.2 Message a group

To message a group, add the group to the messaging conversation via



the 'People' tab.

8.11 Rallypoints

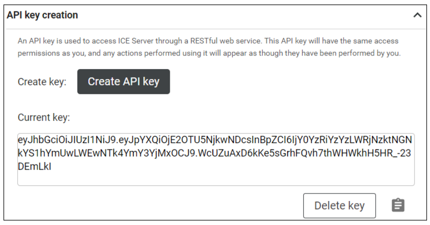
> **Notes:**
>
> - When doing a fresh installation, initial Rallypoints are created and registered automatically.
> - When a Rallypoint is deleted via ICE Desktop, whether intentionally or on accident, it will reappear after ~30 seconds.

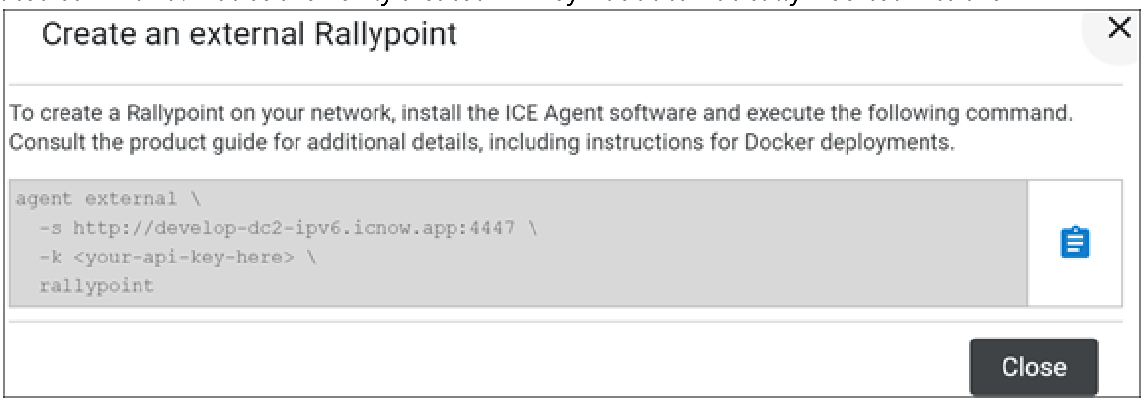
8.11.1 View Rallypoints

Go to 'Settings > Rallypoints > Registered Rallypoints' to see a list of currently registered Rallypoints.

8.11.2 Create a Rallypoint

> **Note:** Creating a Rallypoint requires **ICE Agent** already be installed. ICE Agent is downloadable from the **Instant Connect Support Portal** located at: https://support.instantconnectnow.com/s/downloads.

1. Navigate to Settings > License > Enterprise > API Key Creation. 

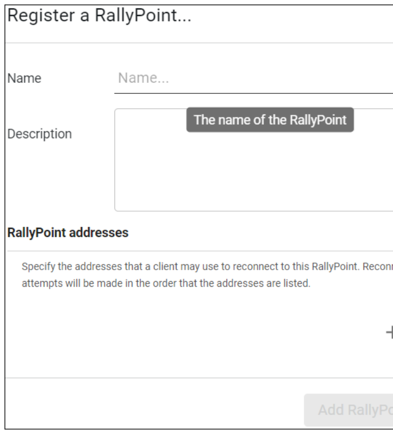
2. Select 'Create API key' and a new API key is automatically generated.
3. Navigate to Settings > Rallypoints.
4. Select '+'.
5. Select 'Create a Rallypoint' to open the 'Create an external Rallypoint' screen, which displays a newly created command. Notice the newly created API key was automatically inserted into the command. 

   > **Note:** If an API key was not yet created, the command will contain a line stating `-k <your-api-key-here>`.

6. Select the clipboard icon to copy the command, then paste it into a convenient location, e.g., a text file.
7. Close the 'Create an external Rallypoint' screen.
8. Open ICE Agent and execute the newly created command.
9. Return to ICE Desktop and see the new Rallypoint is listed.

8.11.3 Register a Rallypoint

1. Navigate to Settings > Rallypoints.
2. Select '+'.



3. Select 'Register a Rallypoint' to open the 'Create an external Rallypoint' screen.
4. Complete the required fields for the existing Rallypoint being registered.
5. Select 'Add Rallypoint'.
6. See the newly registered Rallypoint is listed.

8.11.4 Update Rallypoint(s) when the ICE Server IP address changes

If the ICE Server IP address is updated, then the following Rallypoint and Channel updates also must be performed:

1. Navigate to Settings > Rallypoints.
2. Delete the relevant Rallypoint(s). After ~30 seconds, the deleted Rallypoint(s) will reappear and are automatically updated to reflect the new IP address.
3. Navigate to Settings > Channels.
   - 'Assigned channel defaults' / 'Intercom channel defaults' / 'Telephony defaults': Update to the correct Rallypoint (i.e., with the updated IP address). This ensures the updated Rallypoint is used by default.
   - 'Assigned channels': Update all relevant assigned channels to the updated Rallypoint using the 'Edit' function. This ensures the updated Rallypoint is used by the associated channels.

8.12 Radio Interoperability

The **Radio Interoperability** category contains configuration options for DFSI Gateways, Fixed Stations, ISSI Gateways, and Radio Systems.

8.12.1 P25 Interoperability

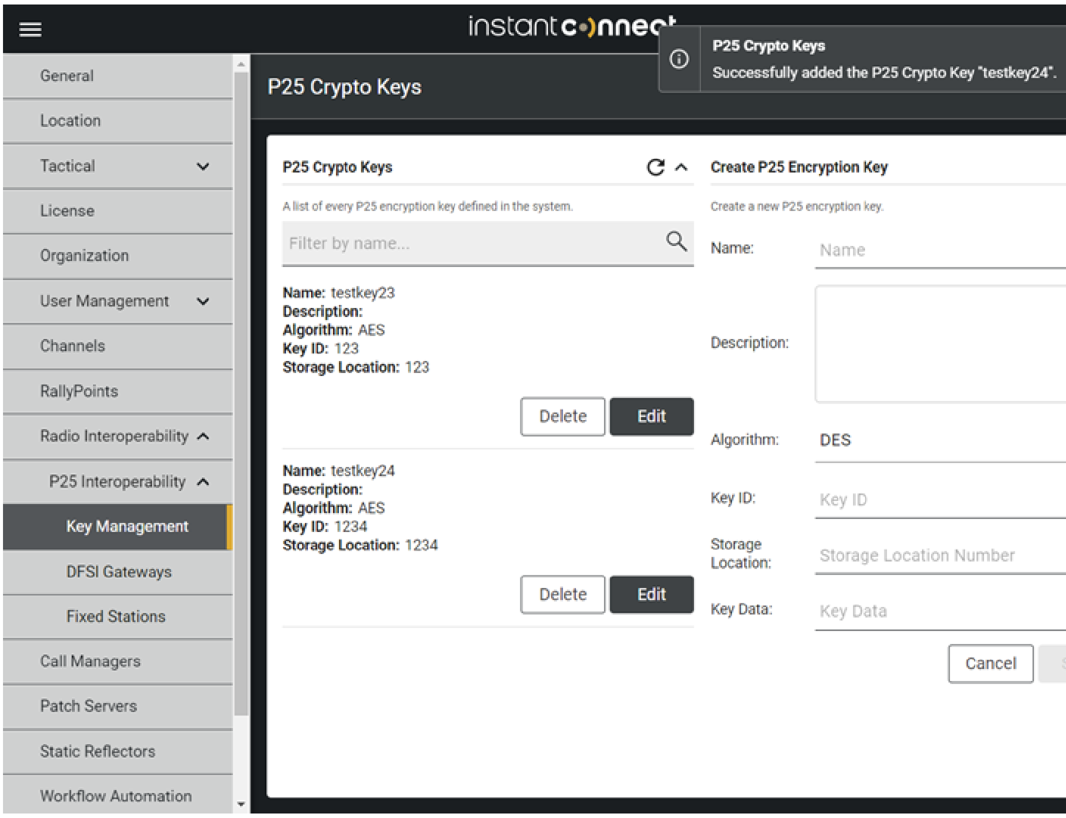
The **P25 Interoperability** category contains P25-specific configuration options for DFSIG and fixed stations.

> **Terms to know:**
>
> - Project 25 (P25): A series of standards and protocols developed by the Telecommunications Industry Association (TIA) TR-8 Committee using open procedures required by the American National Standards Institute (ANSI).
> - Digital Fixed Station Interface (DFSI): A P25 DFSI protocol for connecting conventional P25-base stations or repeaters to local radio communication networks.
> - Fixed Stations (FS): A permanently located radio transmitting station.
> - ICE Radio: A software gateway (DFSIG) connecting ICE Server and P25 DFSI-capable fixed stations. Please see the ICE Radio Administration Guide for more information.
> - Inter-RF Subsystem Interface (ISSI): A P25 protocol that enables multiple RFSSs to be connected together.
> - ISSI Radio System: An external P25 Radio System with RFSS, or an external ISSIG.
> - RFSS: Radio Frequency Subsystem. A basic element in the network infrastructure of a P25 system.

8.12.1.1 Key Management The Key Management screen allows for the the management (i.e., create, edit, delete) of P25 encryption keys.

> **Note:** Any key associated with the channel of a fixed station must be created in the desktop client

> and cannot be imported.



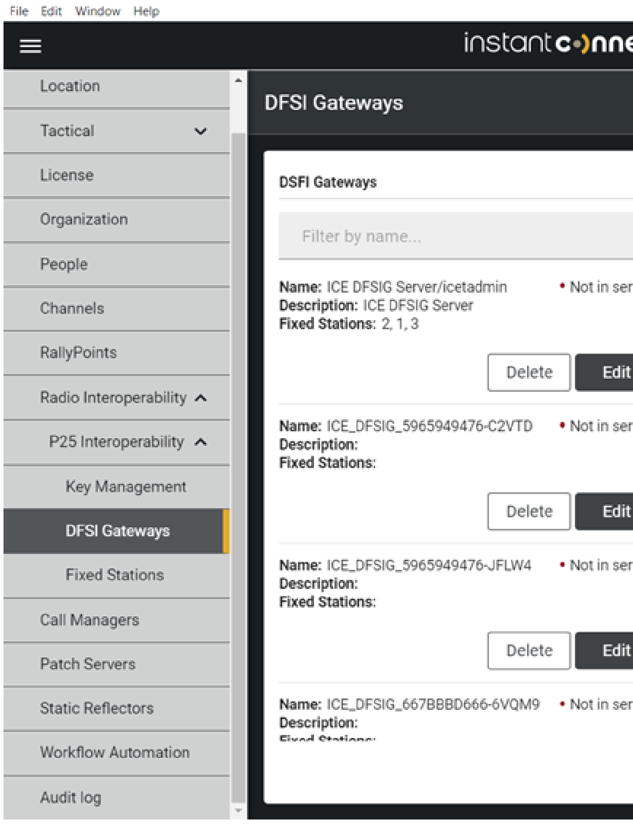
8.12.1.1.1 Create a P25 encryption key

1. Navigate to the 'Create P25 Encryption Key' panel located at Settings > Radio Interoperability > P25 Interoperability > Key Management.
2. Enter the required information.
3. Select the 'Save' button.
4. A banner will display: 

5. On the 'P25 Crypto Keys' panel, you can search for the new key by name.

8.12.1.1.2 DFSI Gateways The **DFSI Gateways** screen allows for the management (i.e., create, edit, delete) of P25 DFSI gateways.

- Indicates whether a gateway is 'in service' or 'not in service'.

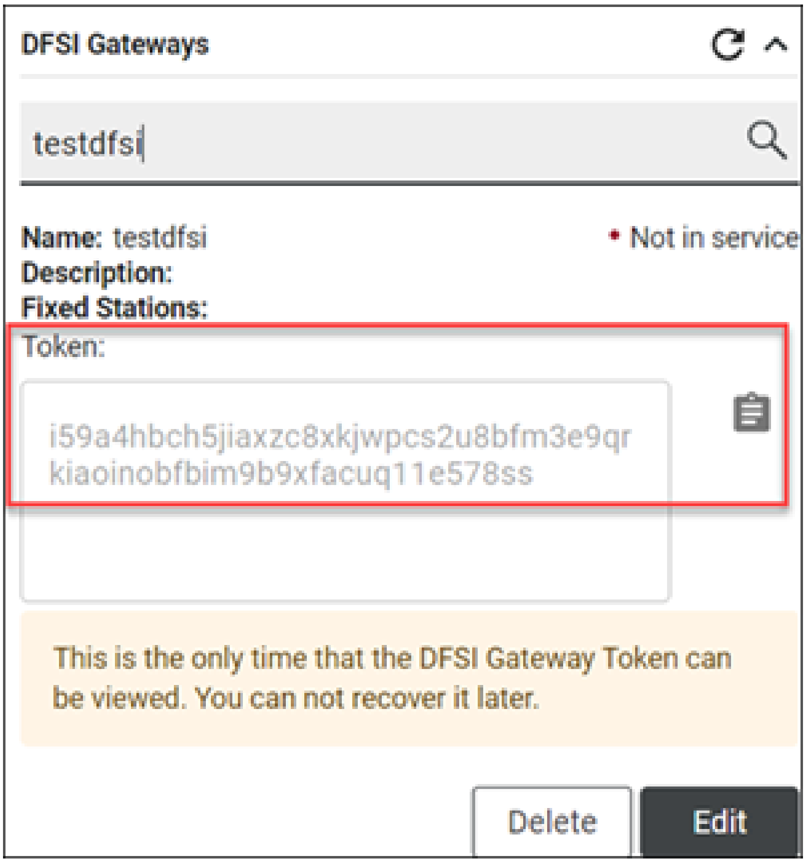


- Lists which fixed stations, if any, are assigned to a gateway.

8.12.1.2.1 Create a DFSI gateway

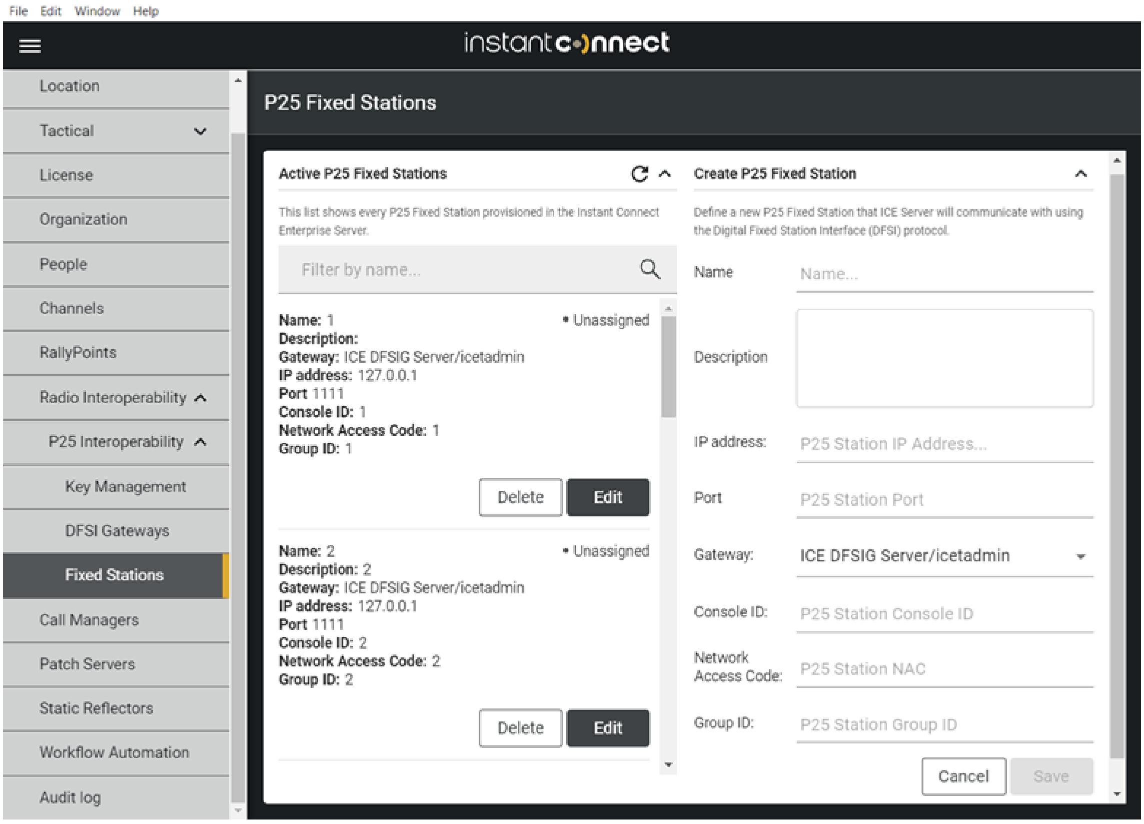
1. Navigate to the 'Create DFSI Gateway' panel located at Settings > Radio Interoperability > P25 Interoperability > DFSI Gateways.
2. Enter the name of the gateway. You can also enter additional descriptive information, if desired.
3. Select the 'Create DFSI Gateway' button.
4. A banner will display: 

5. On the 'DFSI Gateways' panel, search for the new gateway by name.
6. A token code displays in the gateway listing. This is a one-time code that only displays on creation of the gateway, so copy and save it now. Once you navigate away from the 'DFSI Gateway' screen, it will disappear and be irretrievable. Please refer to the **Create an env file** section of the *ICE Radio Administration Guide* for further instructions on using the token code.

   If you do miss the code, then delete the gateway and recreate it, in order to get another one-time code to copy and save. 

8.12.1.3 Fixed Stations The **Fixed Stations** screen allows for the management (i.e., create, edit, delete) of P25 fixed stations.

- Indicates whether a fixed station is assigned to a channel (and which one) or 'unassigned'.



8.12.1.3.1 Create a fixed station and assign it to a channel

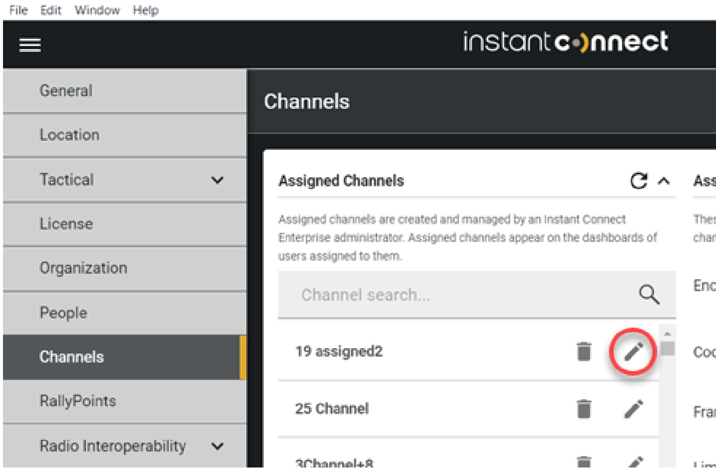
> Fixed stations must be assigned to a channel in order to be available to network users.

1. From the **Fixed Station** screen, under **Create P25 Fixed Station**, populate the required fields:

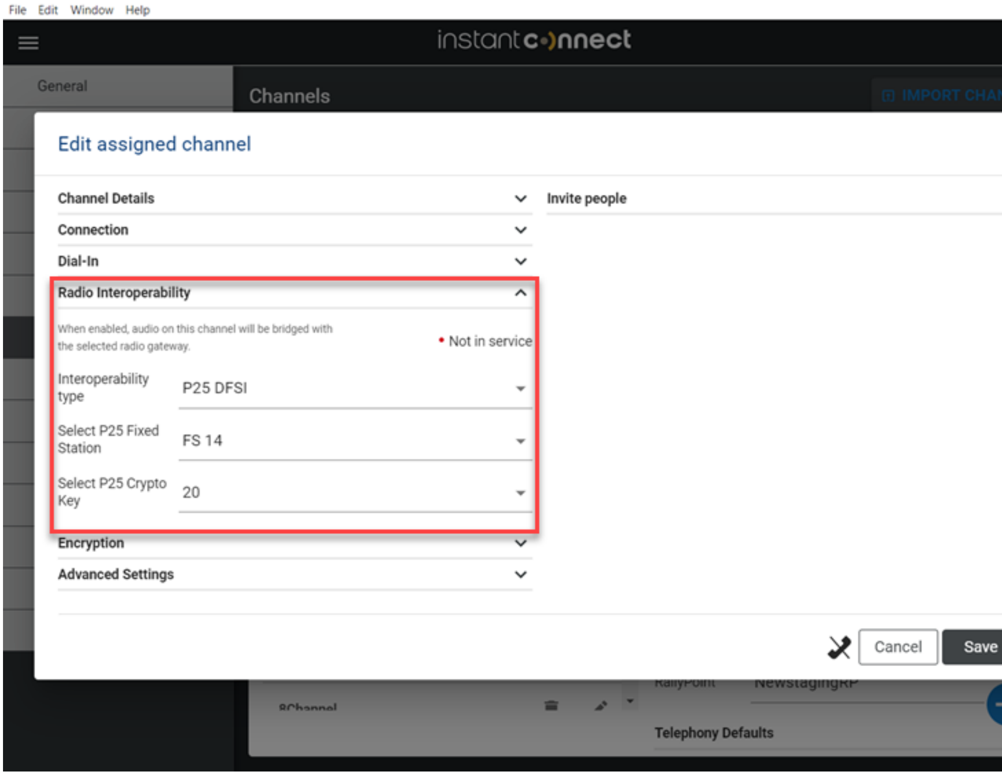
   > Your organization's radio administrator should be able to provide most of these values.

   - Name
   - Host name or IP address
   - Port
   - Gateway (the fixed station is assigned to the gateway specified here)
   - Console ID
   - NAC (Network Access Code)
   - Group ID

2. Select the **Save** button. The new fixed station now appears in the **Active P25 Fixed Stations** list.



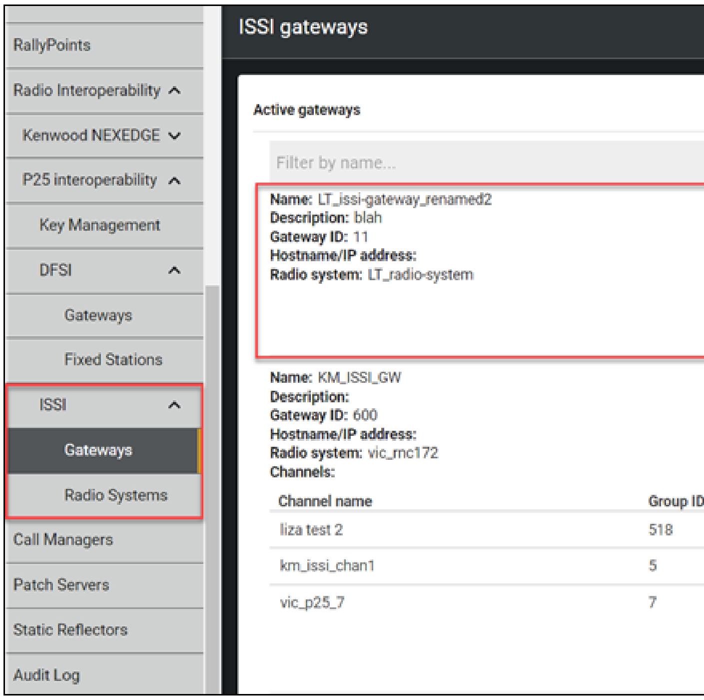
3. From the **Channels** screen, select a channel to edit.
4. From the **Edit assigned channel** popup, under **Radio Interoperability**, populate the required fields.
   - Interoperability type
   - Select P25 Fixed Station (the specified fixed station is assigned to the channel)



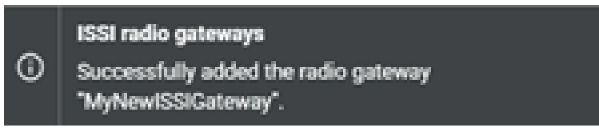
   - Select P25 Crypto Key
5. Select the **Save** button.

8.12.1.4 ISSI Gateways The **ISSI Gateways** screen allows for the management (i.e., create, edit, delete) of P25 ISSI gateways.

- Indicates whether a gateway is 'in service' or 'not in service'.
- Lists which radio system is designated for a gateway.



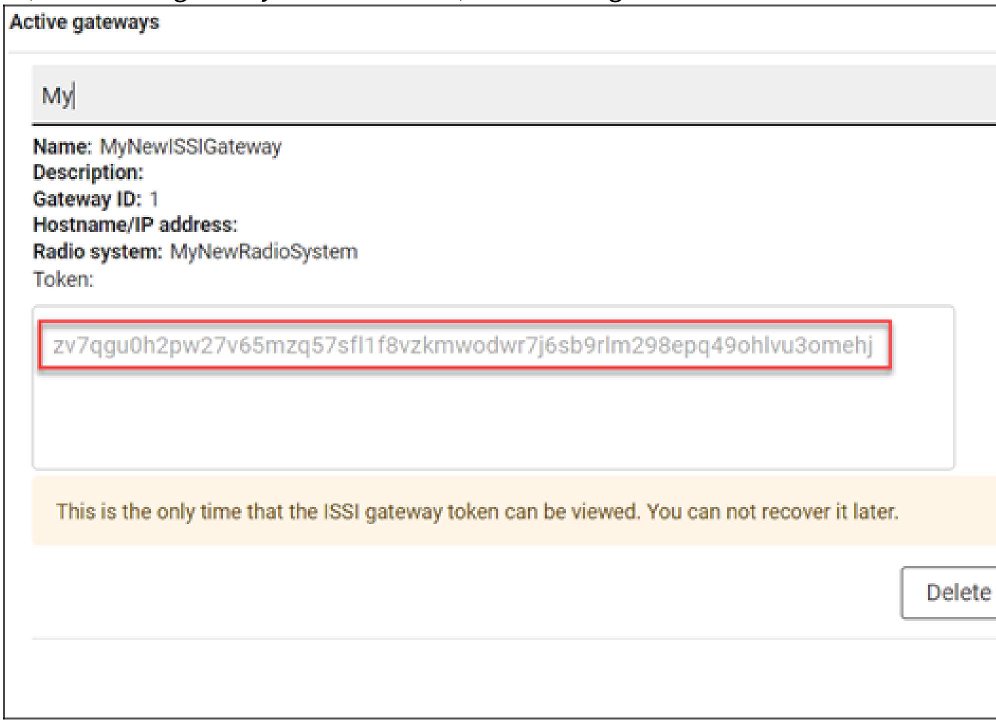
8.12.1.4.1 Create an ISSI gateway

1. When creating an ISSI gateway, an existing radio system must be designated, so, if necessary, first create a radio system by following the instructions in the **Create a radio system and assign it to a channel** section of this document.
2. Navigate to Settings > Radio Interoperability > P25 Interoperability > ISSI > Gateways.
3. Select the + (Create gateway) button in the lower, right of the screen.
4. Enter the gateway name and ID, then select the appropriate radio system. You can also enter additional descriptive information, if desired.
5. Select the 'Create' button.
6. A banner will display confirming the new gateway was added: 

7. On the 'Active Gateways' list, search for the new gateway by name.
8. A token code displays in the gateway listing. This is a one-time code that only displays on creation of the gateway, so copy and save it now. Once you navigate away from this screen, the

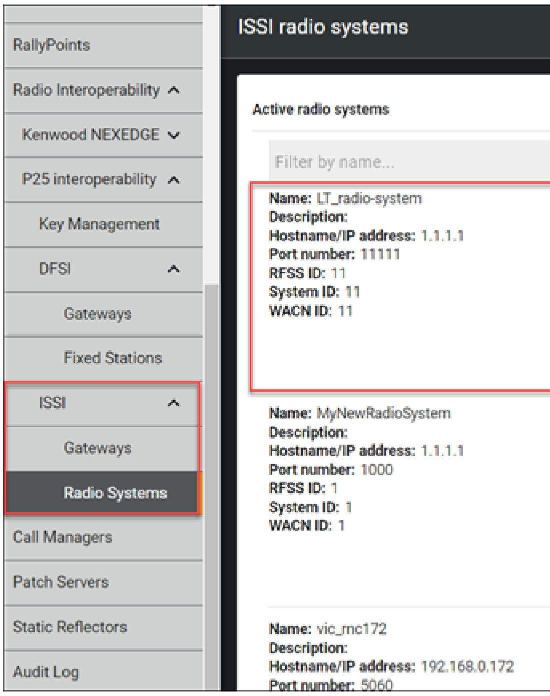
token code will disappear and be irretrievable. Please refer to the **Create an env file** section of the *ICE Radio Administration Guide* for further instructions on using the token code.

If you do miss the token code, delete the gateway and recreate it, in order to get another one-time code to copy and save.



8.12.1.5 Radio Systems The **Radio Systems** screen allows for the management (i.e., create, edit, delete) of P25 radio systems.

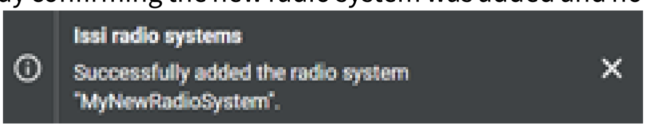
- Indicates whether a radio system is 'connected' or 'disconnected'.

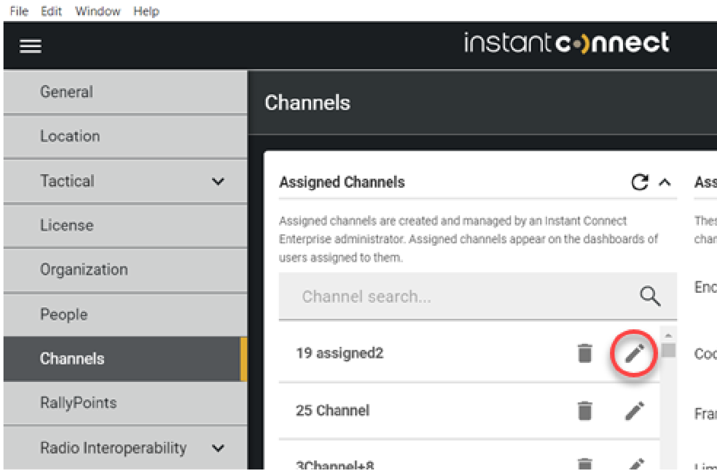


8.12.1.5.1 Create a radio system and assign it to a channel

> **Note:** Radio systems must be assigned to a channel in order to be available to network users.

1. Navigate to **Settings > Radio Interoperability > P25 Interoperability > ISSI > Radio Systems.**
2. Select the + (Create radio system) button in the lower, right of the screen.
3. Populate the required fields. You can also enter additional descriptive information, if desired.
   - Name
   - Description
   - Hostname/IP address
   - Port number
   - RFSS ID
   - System ID
   - WACN ID
4. Select the 'Save' button.
5. A banner will display confirming the new radio system was added and now appears in the active radio systems list.

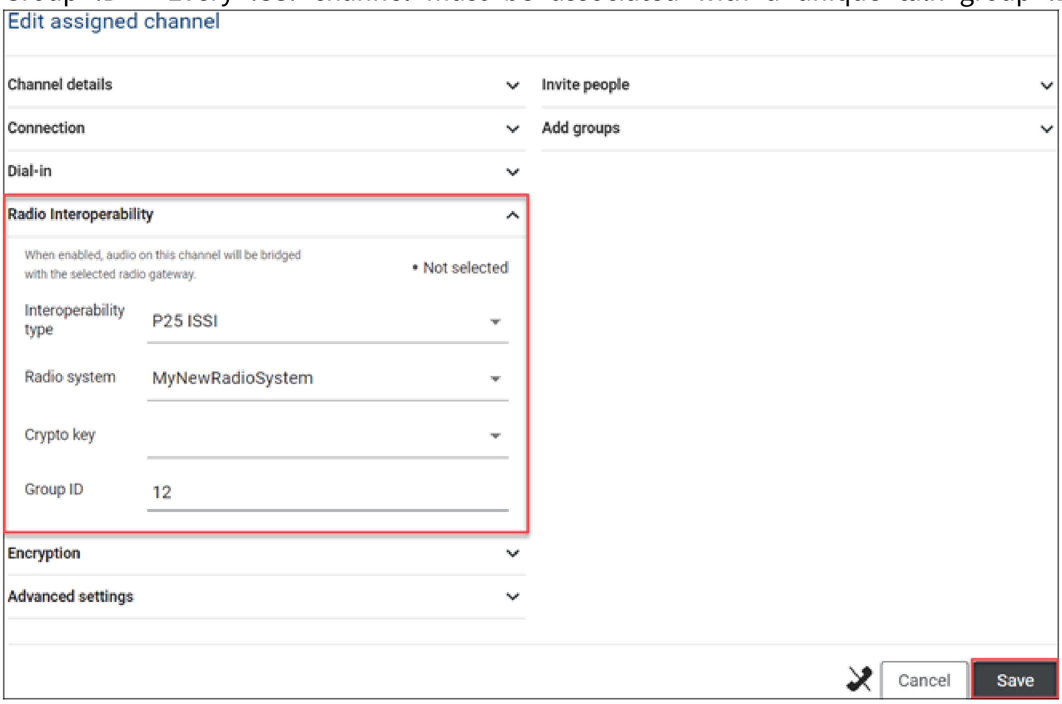




6. From the **Channels** screen, select a channel to edit.

7. From the **Edit assigned channel** popup, under **Radio Interoperability**, populate the required fields.

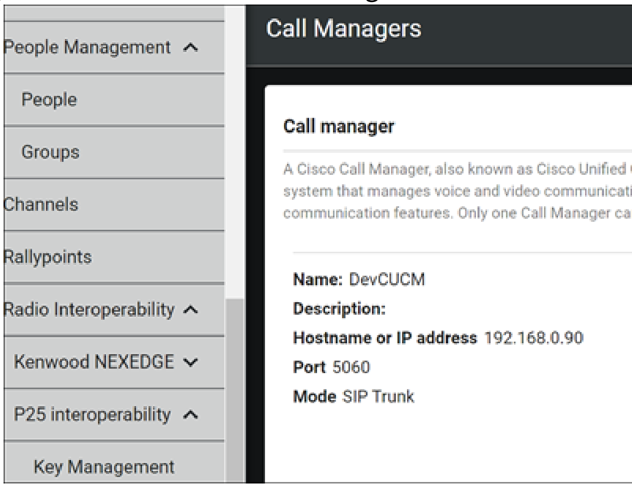
    - Interoperability type = P25 ISSI
    - Radio system = Select the appropriate radio system to assign to the channel.
    - Select P25 Crypto Key = Select as appropriate.
    - Group ID = Every ISSI channel must be associated with a unique talk group ID.



8. Select the **Save** button.

8.13 Call Managers

The **Call Managers** section allows for the configuration, update, and deletion of the call manager for the system, which only allows one call manager to exist at a time.



8.14 Patch Servers

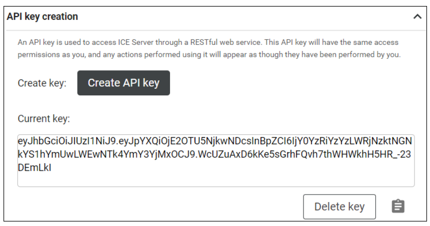
8.14.1 View patch servers

Go to **Settings > Patch Servers > Active patch servers** to see a list of currently active patch servers.

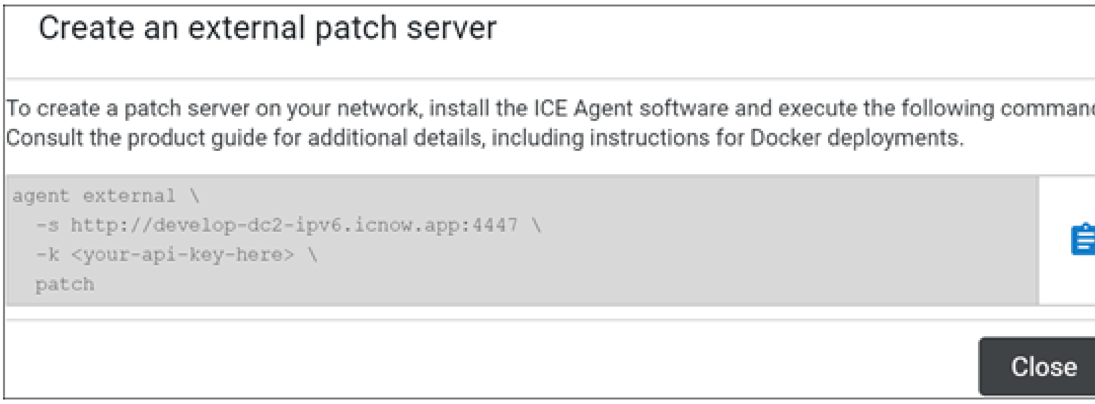
8.14.2 Create a patch server

> **Note:** Creating a patch server requires **ICE Agent** already be installed. ICE Agent is downloadable from the **Instant Connect Support Portal** located at: https://support.instantconnectnow.com/s/downloads.

1. Navigate to **Settings > License > Enterprise > API Key Creation.**



2. Select ‘Create API key’ and a new API key is automatically generated.
3. Navigate to Settings > Patch Servers.
4. Select ‘+’.
5. Select ‘Create a patch server’ to open the ‘Create an external patch server’ screen, which displays a newly created command. Notice the newly created API key was automatically inserted



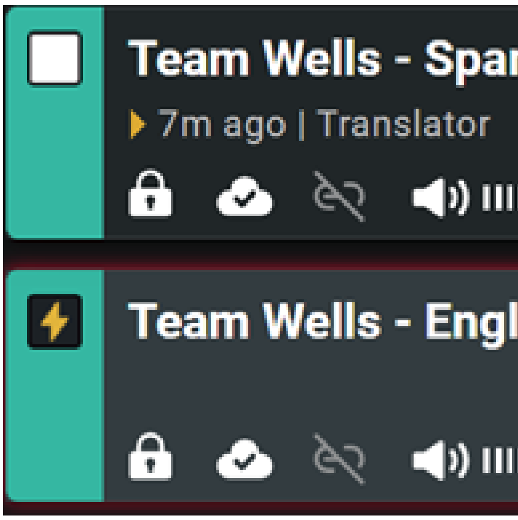
into the command.

> **Note:** If an API key was not yet created, the command will contain a line stating -k <your-api-key-here>.

6. Select the clipboard icon to copy the command, then paste it into a convenient location, e.g., a text file.
7. Close the ‘Create an external patch server’ screen.
8. Open ICE Agent and execute the newly created command.
9. Return to ICE Desktop and see the new patch server is listed.

8.15 Translations

A translation is patch between channels that allows almost real-time translation between people speaking different languages. In the following example a translation patch was created between two channels: one is set to English for its spoken language, and the other is set to Spanish for its spoken language.

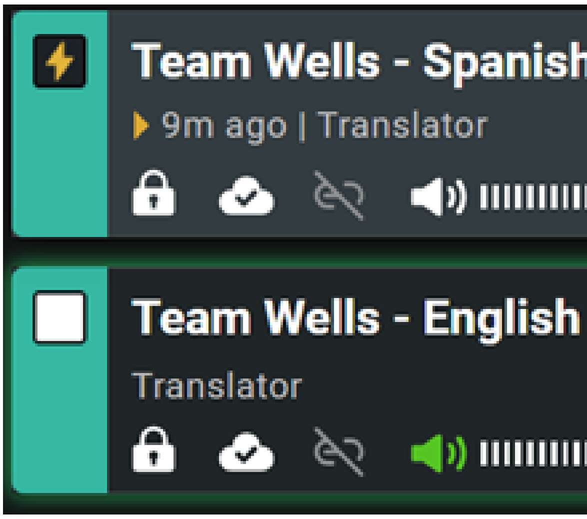


First an English speaker transmits the following, “Hello, can you hear me?”

After a brief pause, the Spanish speakers on the Spanish channel hear, “¿Hola puedes oírme?”

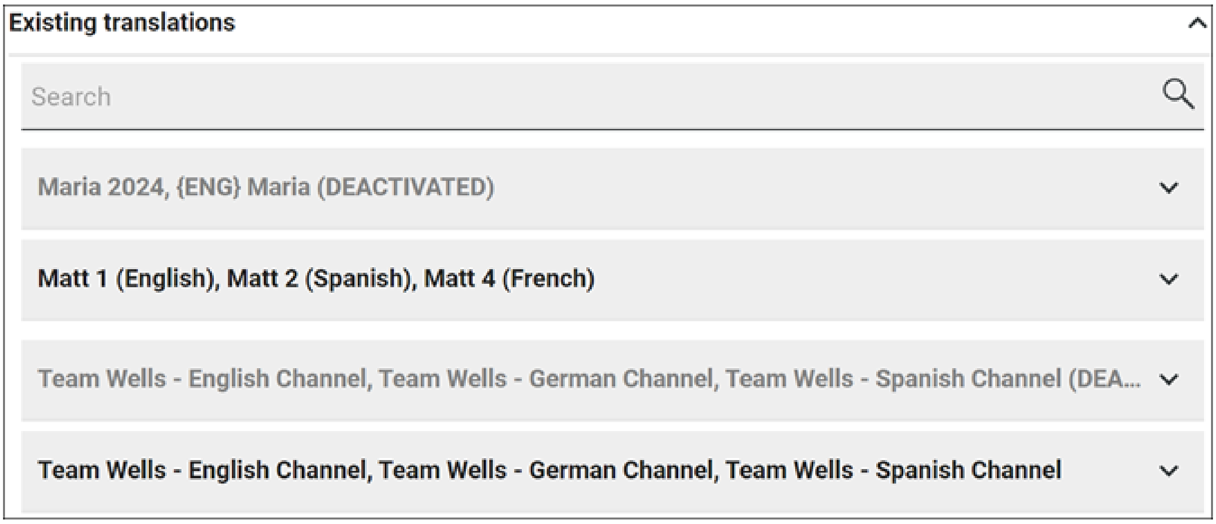
A Spanish speaker then responds, “Sí, podemos oírte.”

After a brief pause, the English speaker hears, “Yes, we can hear you.”



8.15.1 View existing translations

Go to **Settings > Translations > Existing translations.** There a searchable list of translations displays. Activated translations are in **BOLD**, while deactivated translations are marked as such.



8.15.2 Create and activate a translation

> **Note:**
>
> - You must be a Patch Administrator to create and activate translations.
> - Verify the channels to be used are set to different **Spoken Languages** and have **Translation** enabled.

1. Go to Settings > Translations > Create a new translation.
2. Name the translation and add any helpful description.
3. Select the translation server.
4. Select 'Add channels'.
5. Use the search to select at least two channels.
6. Select 'Create'.
7. Select 'Activate'.

8.15.3 Deactivate a translation

1. Go to Settings > Translations > Existing translations.
2. Select the relevant translation.
3. Select 'Deactivate'.
4. The translation will now display as deactivated.

8.15.4 Delete a translation

1. Go to Settings > Translations > Existing translations.

2. Select the relevant translation.
3. Select 'Delete'.
4. The translation is deleted and no longer appears in the list of existing translations.

8.16 Static Reflectors

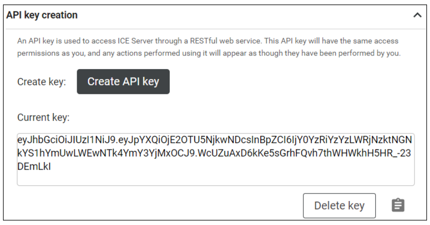
> **Note:** As of ICE 3.3.0, when a static reflector is deleted, whether intentionally or on accident, it will reappear after ~30 seconds.

8.16.1 View active static reflectors

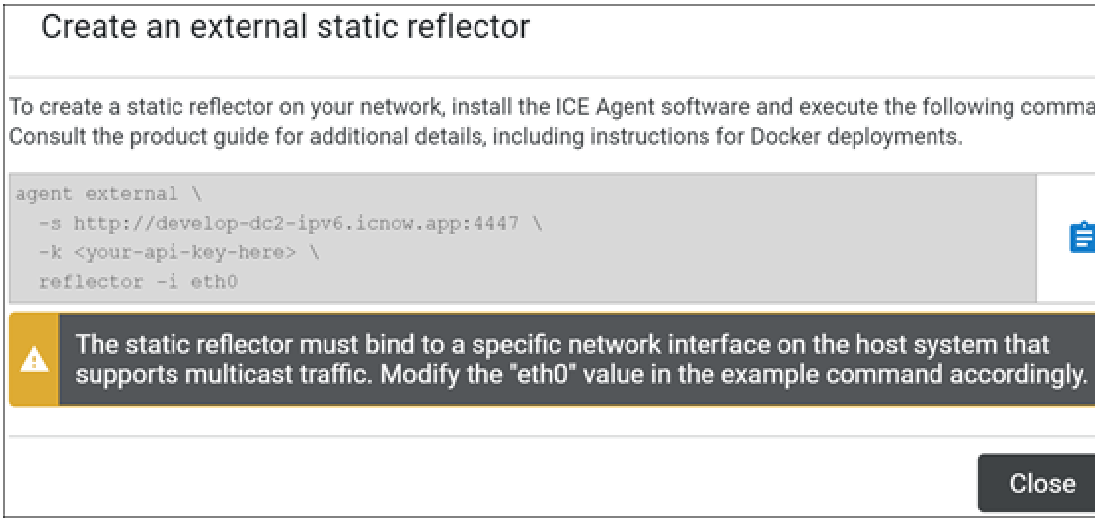
Go to 'Settings > Static Reflectors > Active static reflectors' to see a list of currently active static reflectors.

8.16.2 Create a static reflector

> **Note:** Creating a static reflector requires **ICE Agent** already be installed. ICE Agent is downloadable from the **Instant Connect Support Portal** located at: https://support.instantconnectnow.com/s/downloads.

1. Navigate to **Settings > License > Enterprise > API Key Creation.** 

2. Select 'Create API key' and a new API key is automatically generated.
3. Navigate to Settings > Static Reflectors.
4. Select '+'.
5. Select 'Create a static reflector' to open the 'Create an external static reflector' screen, which displays a newly created command. Notice the newly created API key was automatically inserted



into the command.

> **Note:** If an API key was not yet created, the command will contain a line stating -k <your-api-key-here>.

6. Select the clipboard icon to copy the command, then paste it into a convenient location, e.g., a text file.
7. Close the 'Create an external static reflector' screen.
8. Open ICE Agent and execute the newly created command.
9. Return to ICE Desktop and see the new static reflector is listed.

8.17 Workflow Automation

Workflow Automation provides the ability for users provisioned as Workflow administrator to create Workflow Automation Rules of procedures organized by an "Event" as the trigger and an "Action" that is assigned to the event to be executed when the trigger is received.

8.17.1 Events

Workflow Automation Rules "Events" are the trigger point that will cause the assigned "Action" to be executed.

List of Events that can be used in the creation of Workflow Automation Rules:

- Geofence - Execute the Action when provisioned users enter or leave the geofence boundary.
- On Date/Time - Execute the Action once at the specified Date and Time.
- Scheduled Event / Recurrence - Execute the Action every Minute, Hour, Daily, Weekly, Monthly.
- Webhook - Execute the Action when a request is received on the configured server URL.

8.17.2 Actions

Workflow Automation Rules "Actions" are the list of items that will executed when an "Event" is triggered.

List of Actions that can be assigned to an Event in the creation fo Workflow Automation Rules:

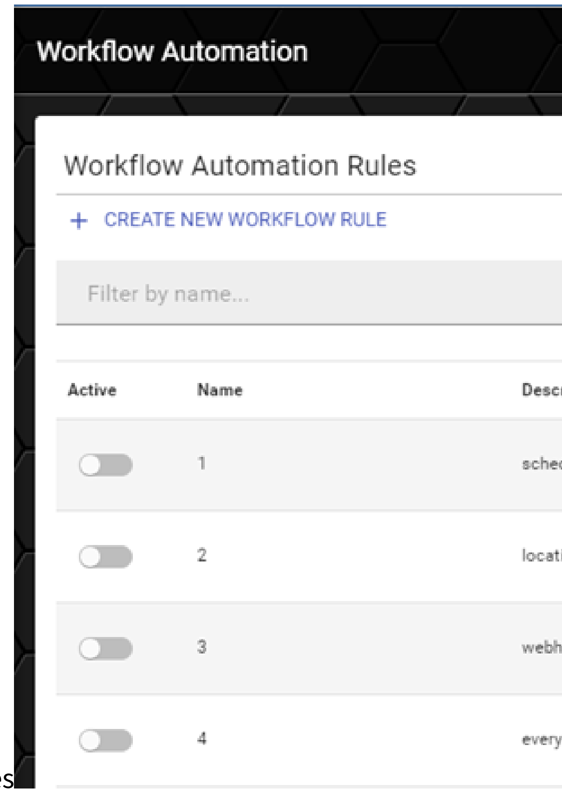
- Create Intercom Channel - Create a temporary channel between a list of users.
- Delete Channel - Delete a Intercom or Assigned channel.
- Assign People to Channel - Assign a list of users to a channel.
- Remove People From a Channel - Remove a list of users from a channel.
- Send Alert Message - Send an alert message to a list of users or on a channel.

8.17.3 Create Workflow Automation Rules

To create a Workflow Automation rule your user account needs to be provisioned as a Workflow Administrator.

Select the Workflow Automation tab from the Settings Menu.

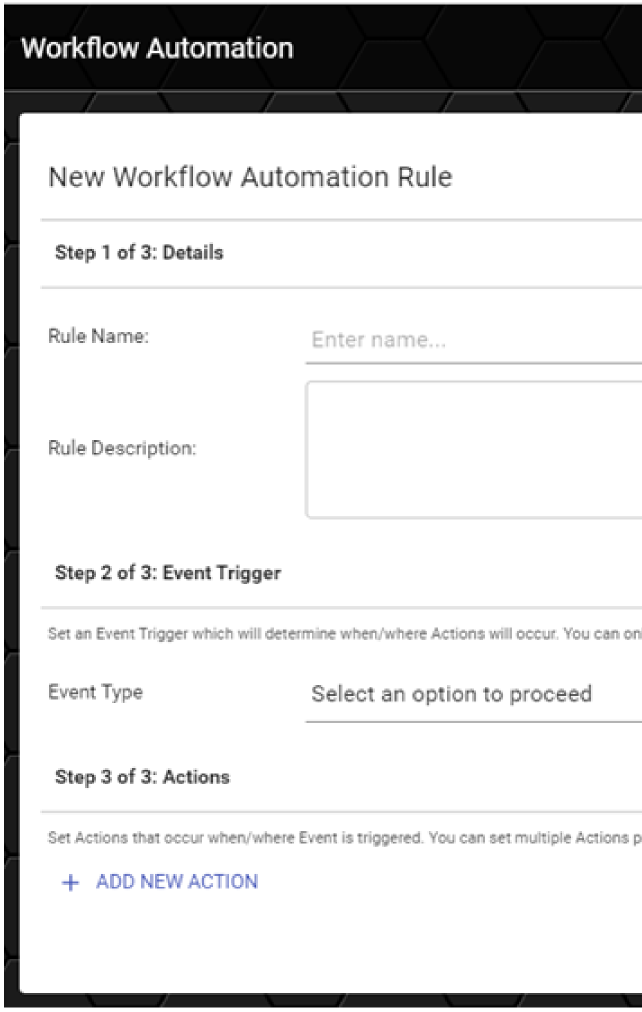
If you do not have the **Workflow Automation** option in your menu contact your System Administrator.



The Workflow Automation page displays a list of created Workflow Rules

Click on the **CREATE NEW WORKFLOW RULE** button to open the **New Workflow Automation Rule** form.

8.17.4 New Workflow Automation Rule Form



The New Workflow Automation Rule form is divided into 3 steps:

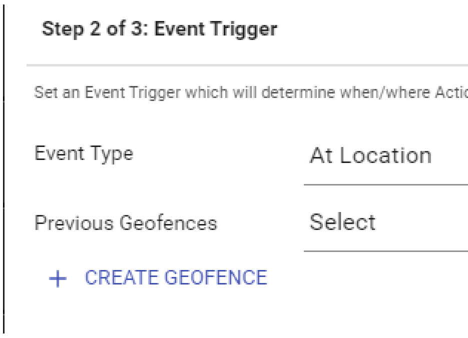
1. **Details:** Enter a Name and a Description of the rule you are creating. The Name and Description is displayed in the list of Workflow Automation Rules.
2. **Event Trigger Type:** From the drop down list select the type of Event Trigger that will be used to start the Actions configured in this Workflow.
    - **At Location** - Execute the Action when provisioned users enter or leave the geofence boundary
    - **On Date/Time** - Execute the Action once at the specified Date and Time

- Via Webhook - Execute the Action when a request is received on the configured server URL

3. **Actions** - Add the action that you want to have execute on the receipt of the Event Trigger.

8.17.5 Event Triggers

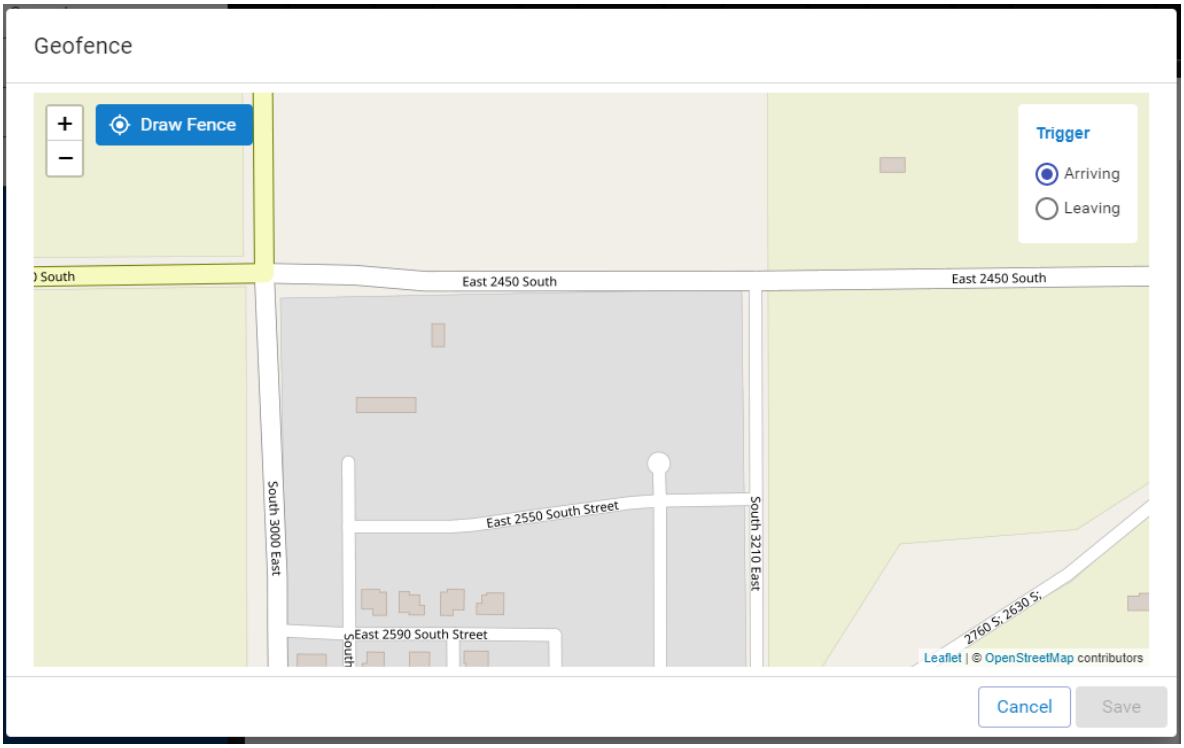
8.17.5.1 At Location Trigger (Geofence) The **At Location** Event Trigger is used to create a Workflow Automation Rule that triggers the Action when users assigned to the rule enter or leave the geofence boundary.



Select the **At Location** Event Trigger Type frome the Event Type drop down list.

You can choose to use an existing geofence by selecting a saved geofence from the Previous Geofences list.

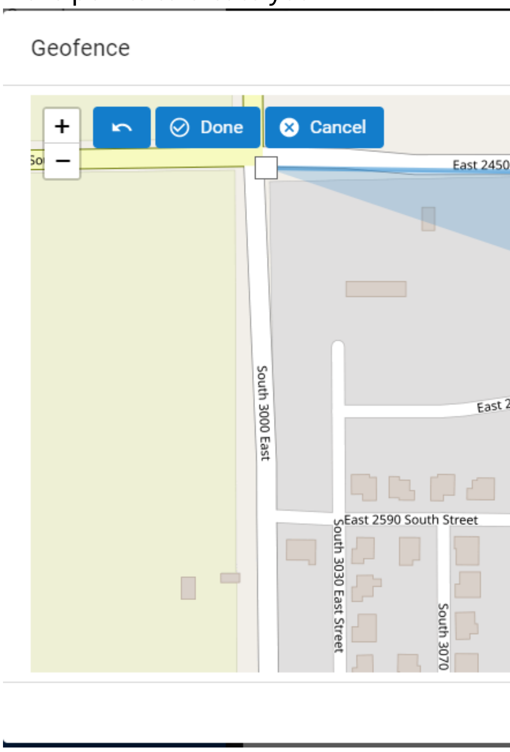
To create a new geofence click on the **CREATE GEOFENCE** button. The Geofence map opens, allowing you to select the trigger type (Arriving or Leaving for this geofence), and to zoom into the location for



the geofence.

To draw a geofence boundary, tap the **Draw Fence** button. You can now draw a new boundary.

Tap the starting point of the geofence boundary and drag the size icons on the points to create your

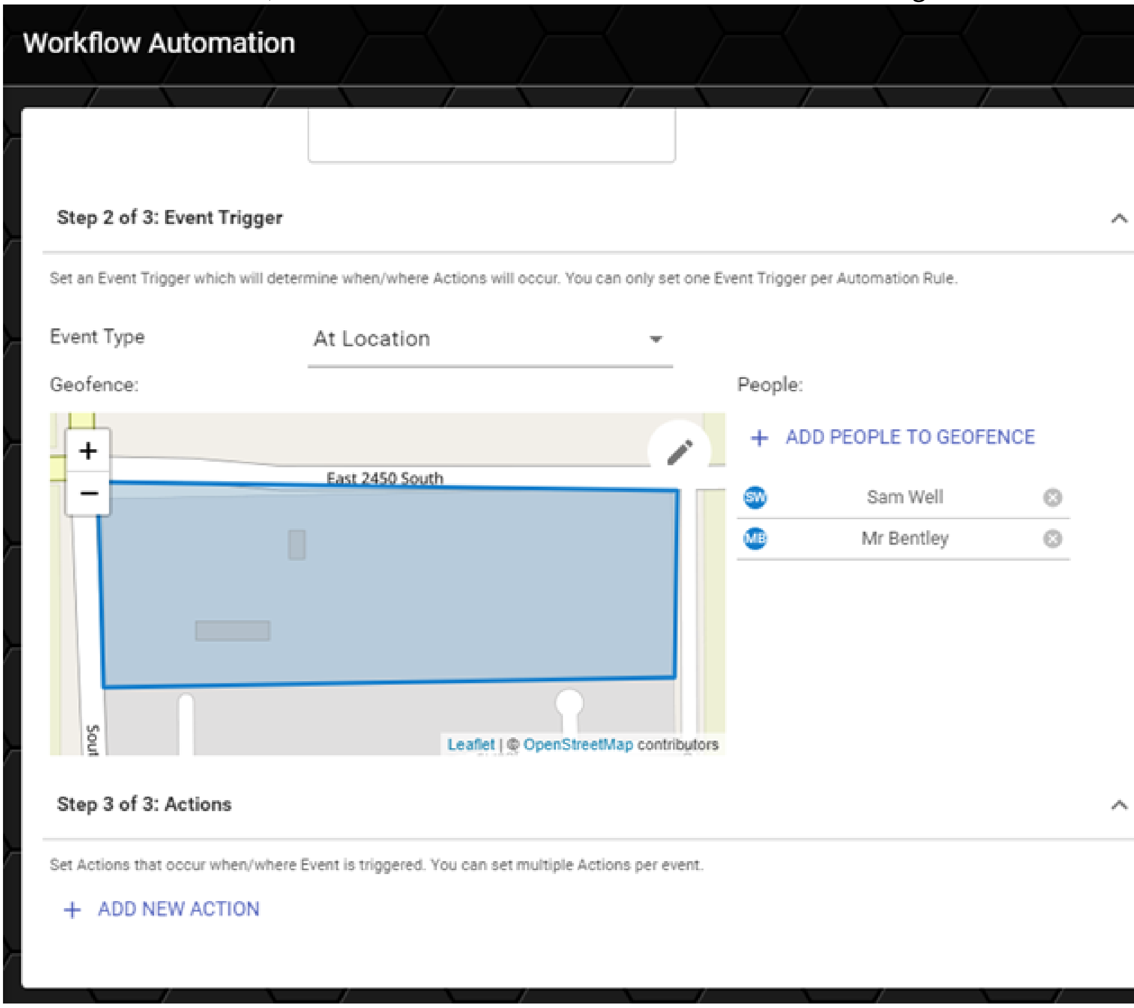


boundary. The shaded area on the map indicates your geofence boundary.

Click the **Save** button to save your geofence boundary.

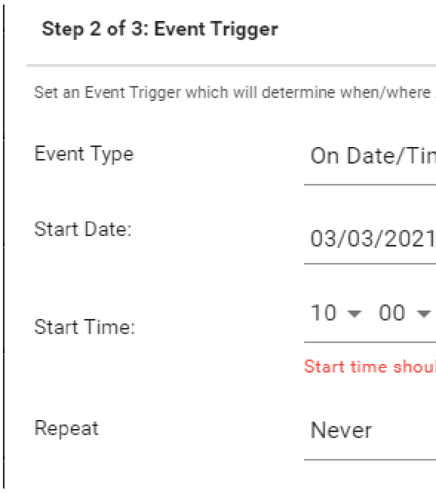
Now that you have created your geofence you need to add users to the geofence that will trigger the event when they enter or leave the geofence.

Click on the **Add People To Geofence** button, select the users from the list of users that will use this geofence and click Save.



The selected users are now added to the At Location Event trigger.

8.17.5.2 On Date/Time Trigger The **On Date/Time** Event Trigger is used to create a Workflow Automation Rule that triggers the Action on the configured Date/Time.

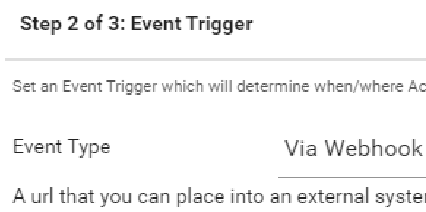


Select the **On Date/Time** Event Trigger Type frome the Event Type drop down list.

Enter the Start Date and Start Time for the Workflow, select how often you what the rule to reoccur from the Repeat drop down list.

8.17.5.3 Via Webhook Trigger

The **Via Webhook** Event Trigger is used to create a Workflow Automation Rule that triggers on a received post to a Webhook.

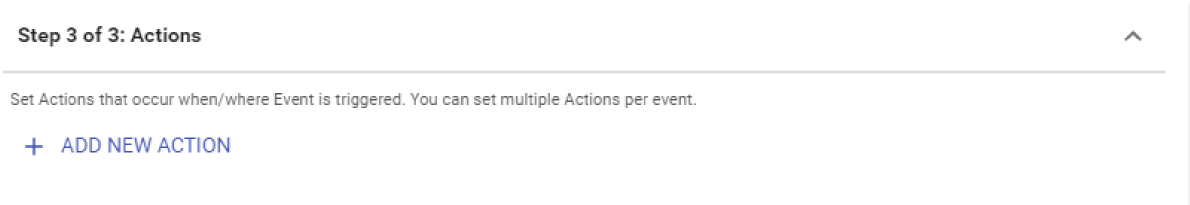


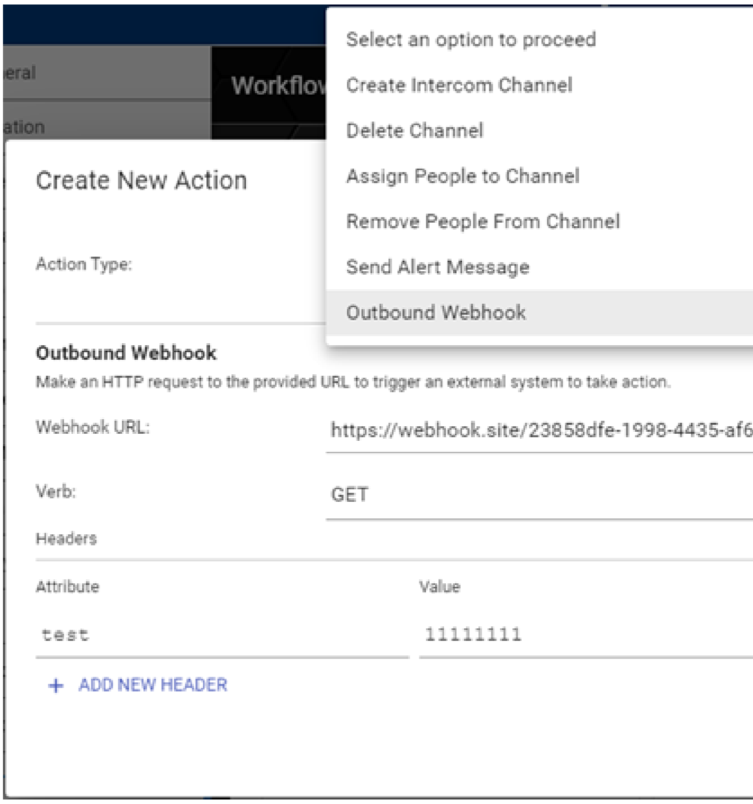
Select the **Via Webhook** Event Trigger Type frome the Event Type drop down list.

Click the Save button to save the Workflow Automation Rule. The Webhook URL is displayed in a dialog box. Use the displayed URL in your system that will be sending the webhook event.

8.17.6 Actions

Actions are a list events that are executed when an Event is triggered.

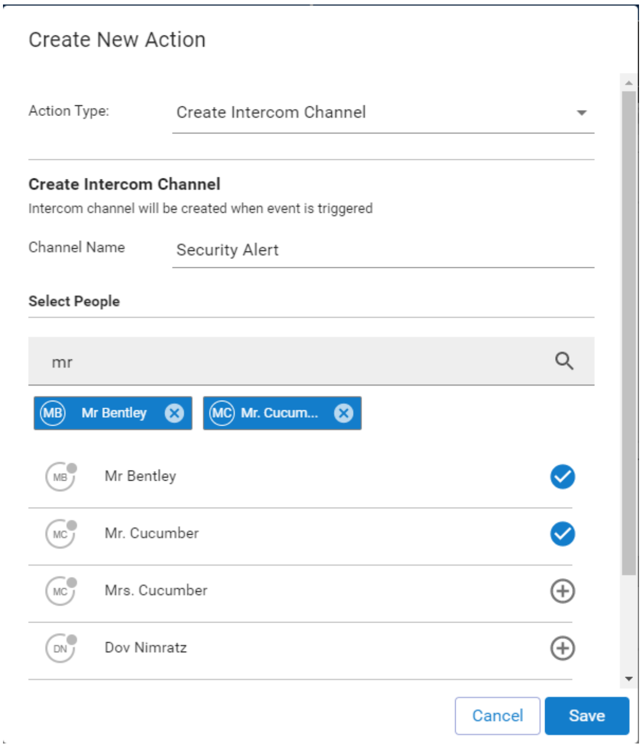




Click the **ADD NEW ACTION** button to create an action.

Select the Action Type from the list in the Create New Action screen.

8.17.6.1 Create Intercom Channel Action The **Create Intercom Channel** action will create a private channel with the users that are assigned to the channel in the action form.



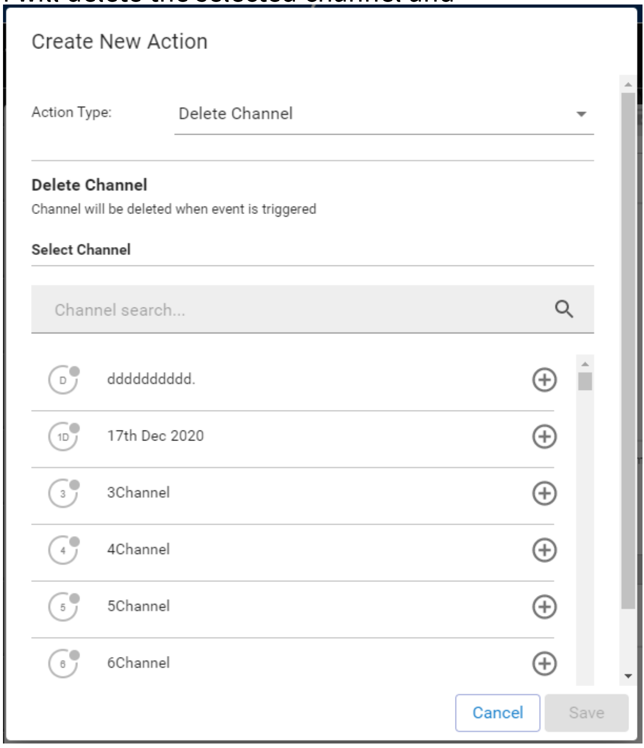
To configure the Create Intercom Channel action select Create Intercom Channel from the Action type list.

1. Enter a name for the channel and select People from the list of users. Use the search filter to find users in the list.

2. When all the users have been assigned click on the Save button.

In this example the channel name is **Security Alert** and will be assigned to the users **Mr Bentley** and **Mr Cucumber**.

8.17.6.2 Delete Channel Action The **Delete Channel** action will delete the selected channel and

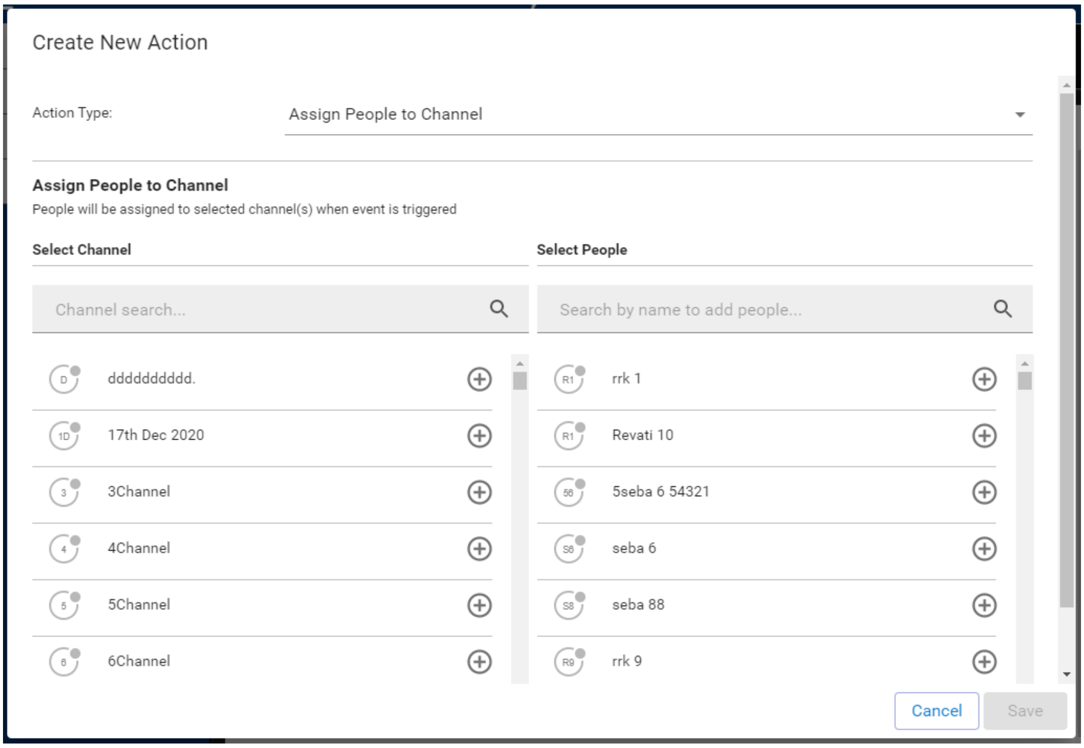


remove it from all users that have been assigned to the channel.

To create the Delete Channel action select Delete Channel from the Action type list.

1. Select the channel from the list of channels or use the search filter to find the channel you want deleted and click on the plus sign button to select it.

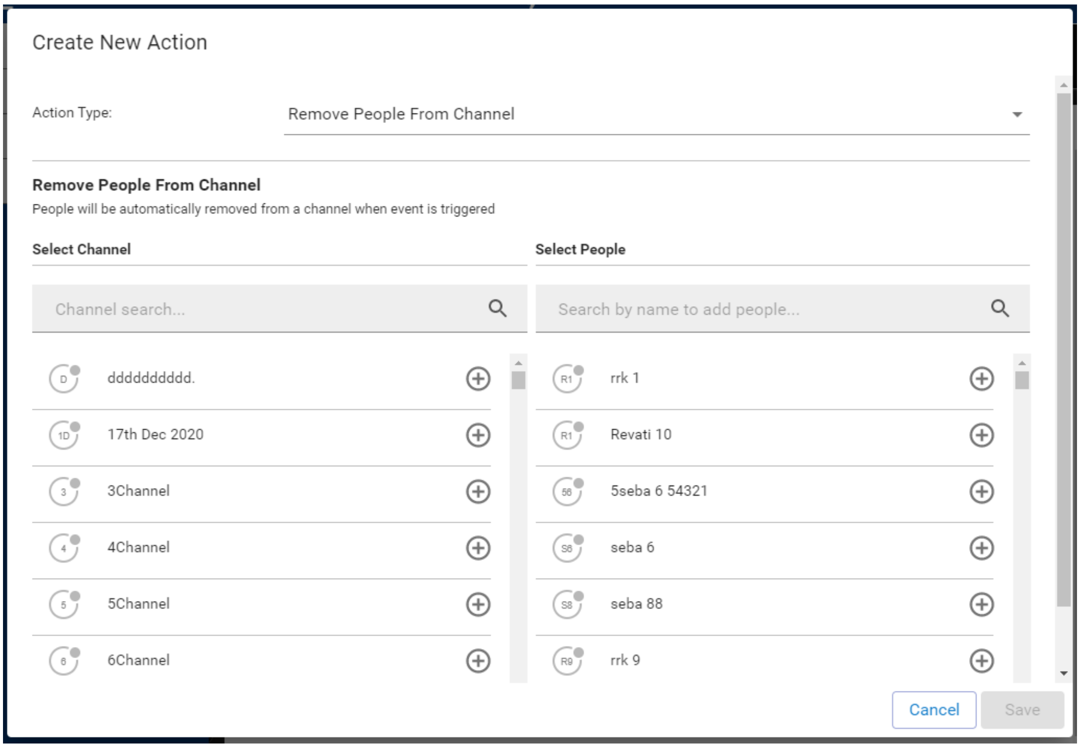
2. Click on the Save button.

8.17.6.3 Assign People to Channel Action The **Assign People to Channel** action will assign the list of users to the selected channel. The channel will appear on the users client as a new resource to use. 

To add people to a channel in the action select Add People to Channel from the Action Type list.

1. Select the channel from the list of channels or use the search filter to find the channel you want assigned to the users click on the plus sign button to select it. Then select the users from the list of users or use the search filter to find the users you want to add to the channel and click on the plus sign button to select them.
2. Click the Save button.

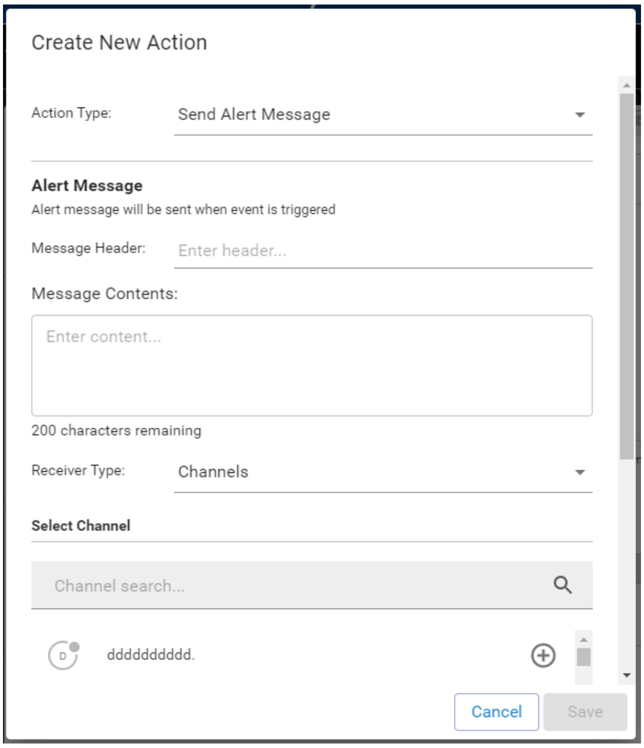
8.17.6.4 Remove People From Channel Action The **Remove People From Channel** action will remove the list of users to the selected channel. The channel will disappear on the users client as a re-



source to use.

To remove people from a channel in the action select Remove People From Channel from the Action Type list.

1. Select the channel from the list of channels or use the search filter to find the channel you want remove the assigned users from and click on the plus sign button to select it. Then select the users from the list of users or use the search filter to find the users you want to remove from the channel and click on the plus sign button to select them.
2. Click the Save button.

8.17.6.5 Send Alert Message Action The **Send Alert Message** action will send an alert message on the selected channel. All users assigned to the channel will receive the Alert Message. Users that are online will receive the message immediately. Users that are offline will receive the message on a successful login. 

To send an alert message on a channel or to a list of users select Send Alert Message from the Action Type list.

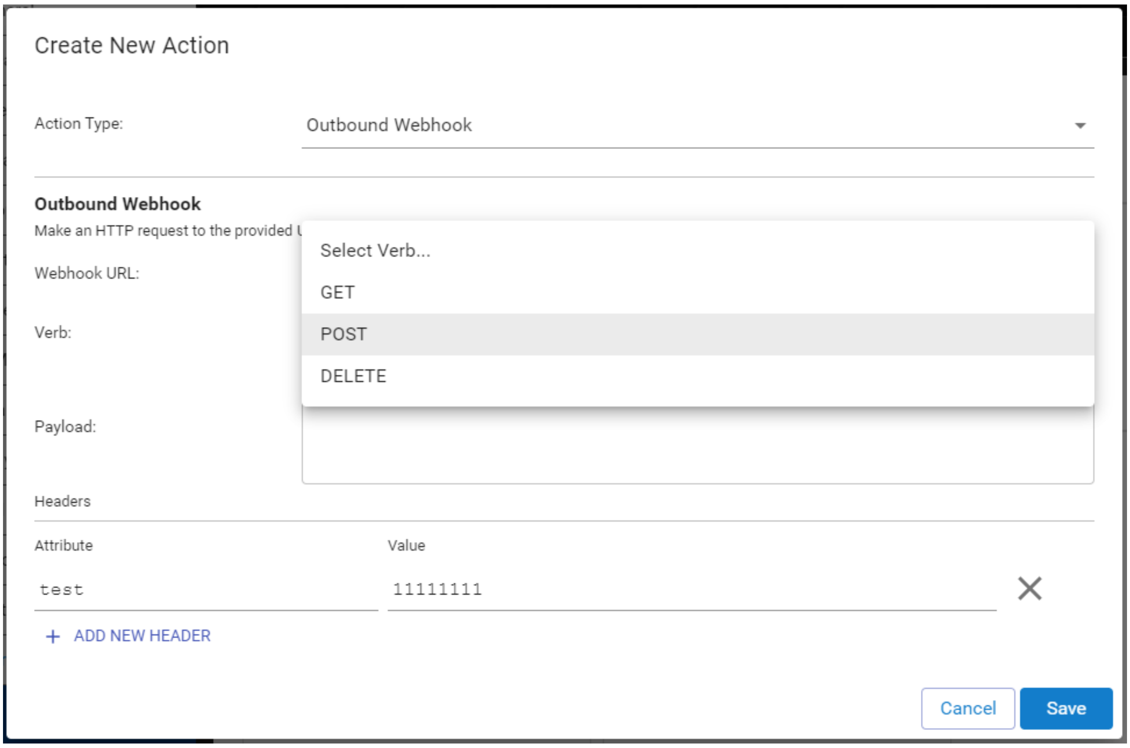
1. Enter the Message Header for the Alert Message in the Message Header field. Type the complete Alert Message in the Message Contents box.

2. To send the message to all users on a list channels, select Channels from the **Receiver Type** and select the channels from the list of channels or use the search filter to find the channels you want to send the alert message on and click on the plus sign button to select each channel.

3. To send the message to a list users select Persons from the **Receiver Type** and select the users from the list of userss or use the search filter to find the users you want to send the alert message to and click on the plus sign button to select each user.

4. Click the Save button.

8.17.6.6 Outbound Webhook Action The **Outbound Webhook** action will send a request to the configured URL for the webhook. The post to the webhook URL will invoke the action on the external system. The action can be used to start another event on the external system, generate a query for data or any other action that can be implemented on the system you are integrating with.

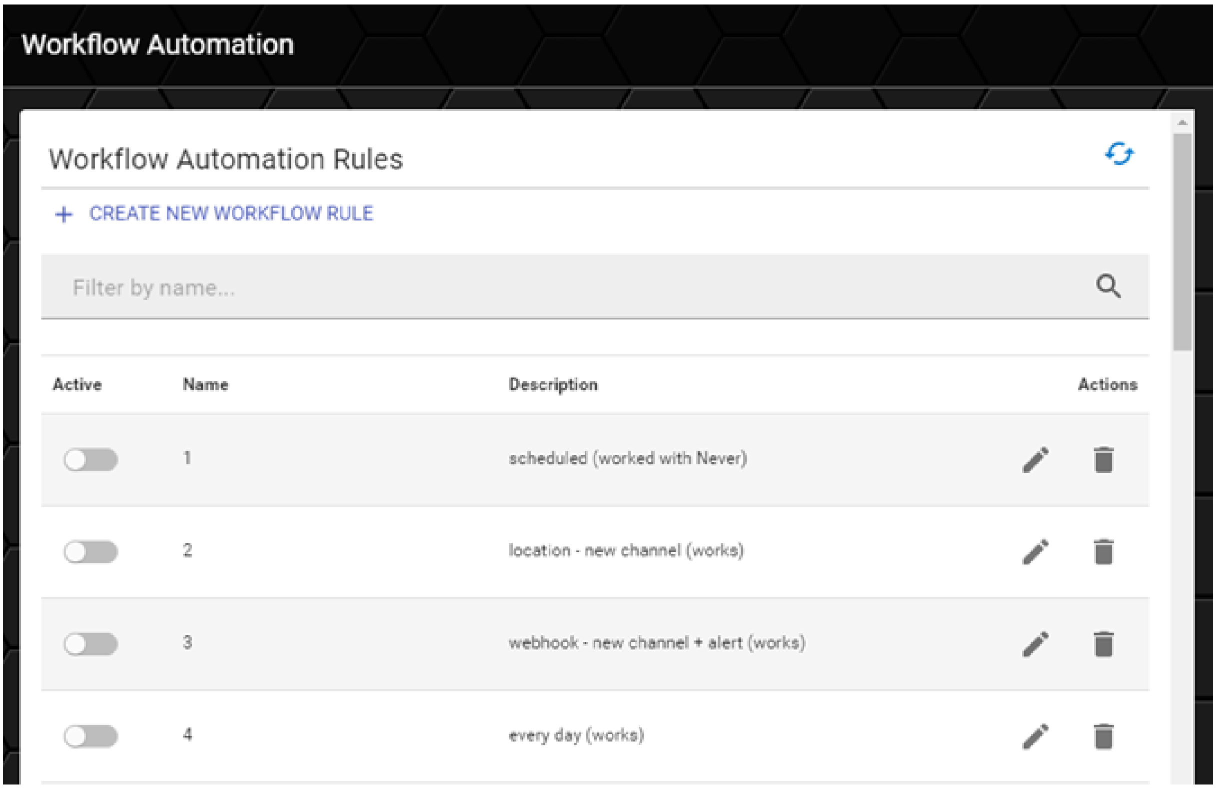


To make an Outbound Webhook request to an webhook URL select Outbound Webhook from the Action Type list.

1. Enter the complete URL in the Webhook URL field.
2. Select the verb / method to be used in the webhook request: Get, Post or Delete.
3. Type any payload information into the Payload box.
4. Enter required Header Attribute / Value pairs in the list.
5. Click the Save button.

8.17.7 Activating a Workflow Automation Rule

Workflow Automation Rules can be Activated or Deactivated from the Workflow Automation Rule list.

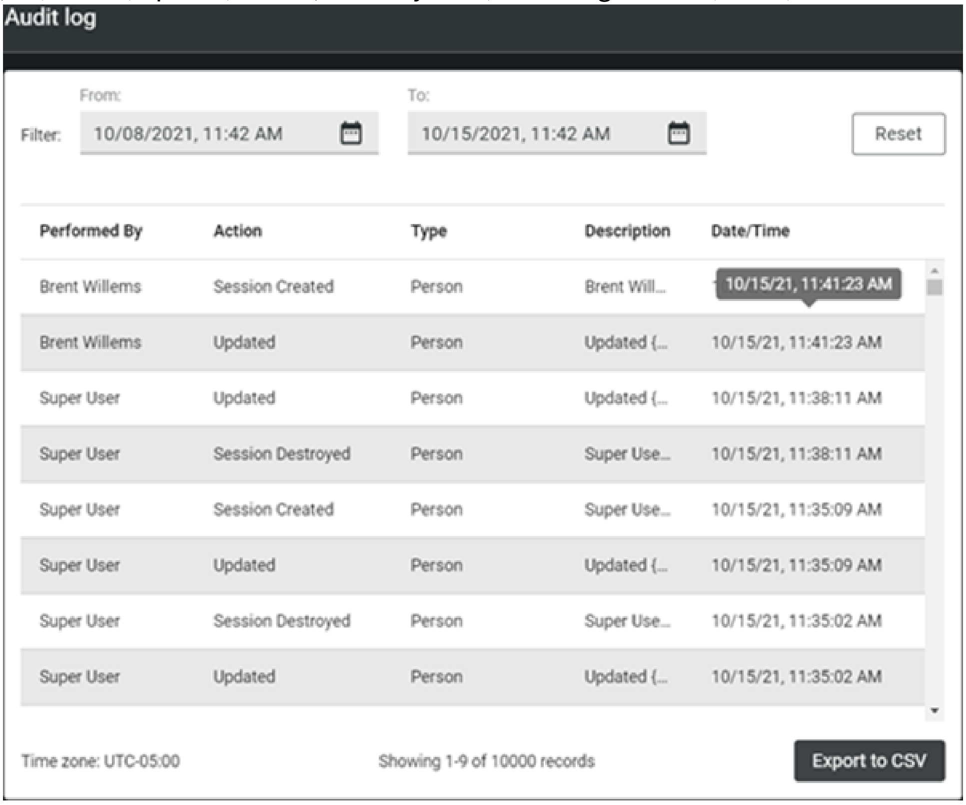


To Activate a Workflow Automation Rule click the Enable / Disable button on the rule you want to activate.

The Enable / Disable button will turn blue when the rule is active.

8.18 Audit Log

The audit log records changes (i.e., create, update, delete) to the system, including the who, what, and when in regards to the change.



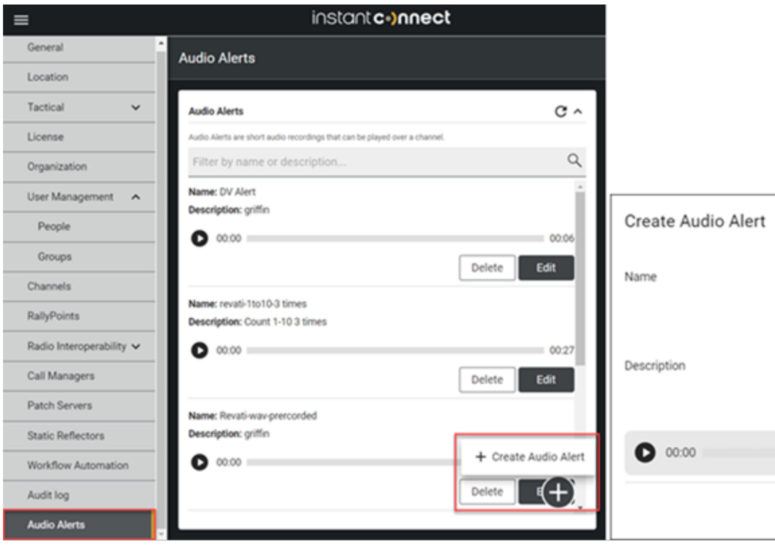
- Filter: The 7-day default timeframe can be modified vi the 'From' and 'To' dates.
- Reset: Select to return the timeframe to the 7-day default.
- Audit record fields:
  - Performed By
  - Action
  - Type
  - Description
  - Date/Time
- Export to CSV: Select to export the audit log records as a .csv file. There is a 10,000 row limit for the exported file.

8.19 Audio Alerts

Audio alerts allow prerecorded audio files to be broadcast over selected channels. The audio files must meet the following specifications:

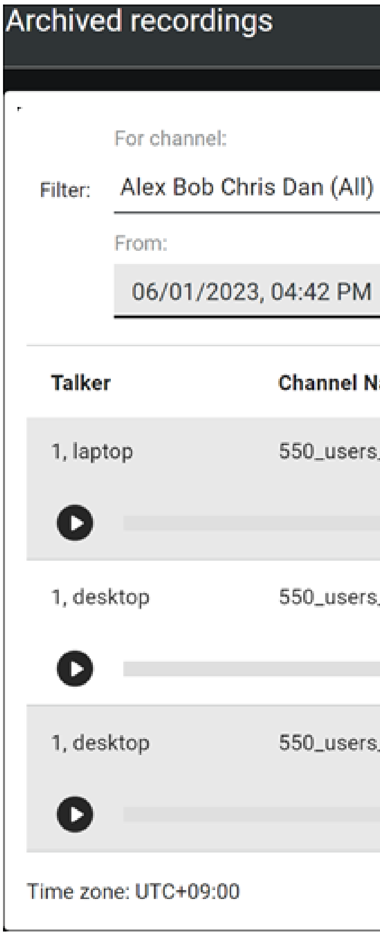
- Duration = 60 seconds or less
- File type = .wav
- File size = 15 MB or less
- Sample rate = 16000 Hz
- Number of channels = 2 (stereo)
- Codec = PCM

8.19.1 Create an audio alert

Record or upload an alert audio file for transmission. 

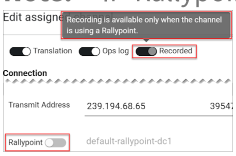
1. Navigate to Settings > Audio Alerts.
2. Select the 'Create Audio Alert' button.
3. Name the alert and attach an audio file:
   - Record a new audio file:
     1. Select the 'Create Recording' button.
     2. Select the record button and speak into your device's microphone.
     3. When done, select the stop button to stop recording.
   - Upload an existing audio file:
     1. Select the 'Upload Recording' button.
     2. From the resulting file search popup, select the relevant audio file.
4. Play the attached audio file to confirm it is ready.
5. Select the 'Create' button. A banner appears: 

9 Archived recordings



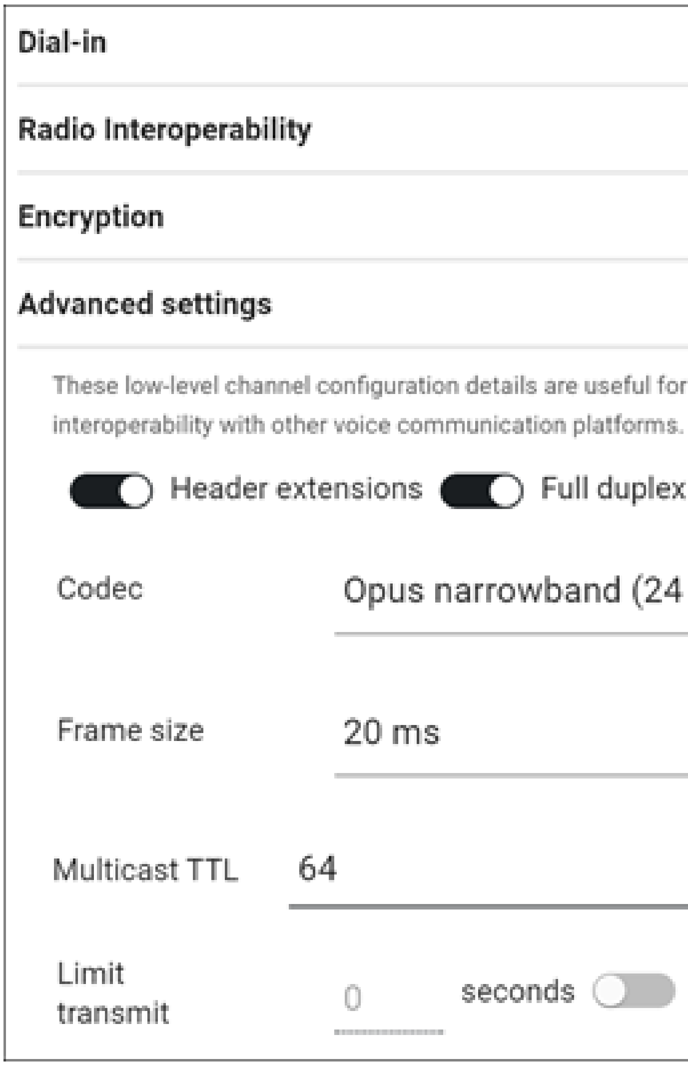
The Archived recordings page provides access to recorded audio communication files.

9.1 Enable recording for a channel

> **Note:** If Rallypoint is disabled for a channel, then Archived Recording is unavailable.
>
> 
>

1. Go to Settings > Channels.
2. Search for the channel.
3. Edit the channel.
4. Go to the 'Advanced settings' section.

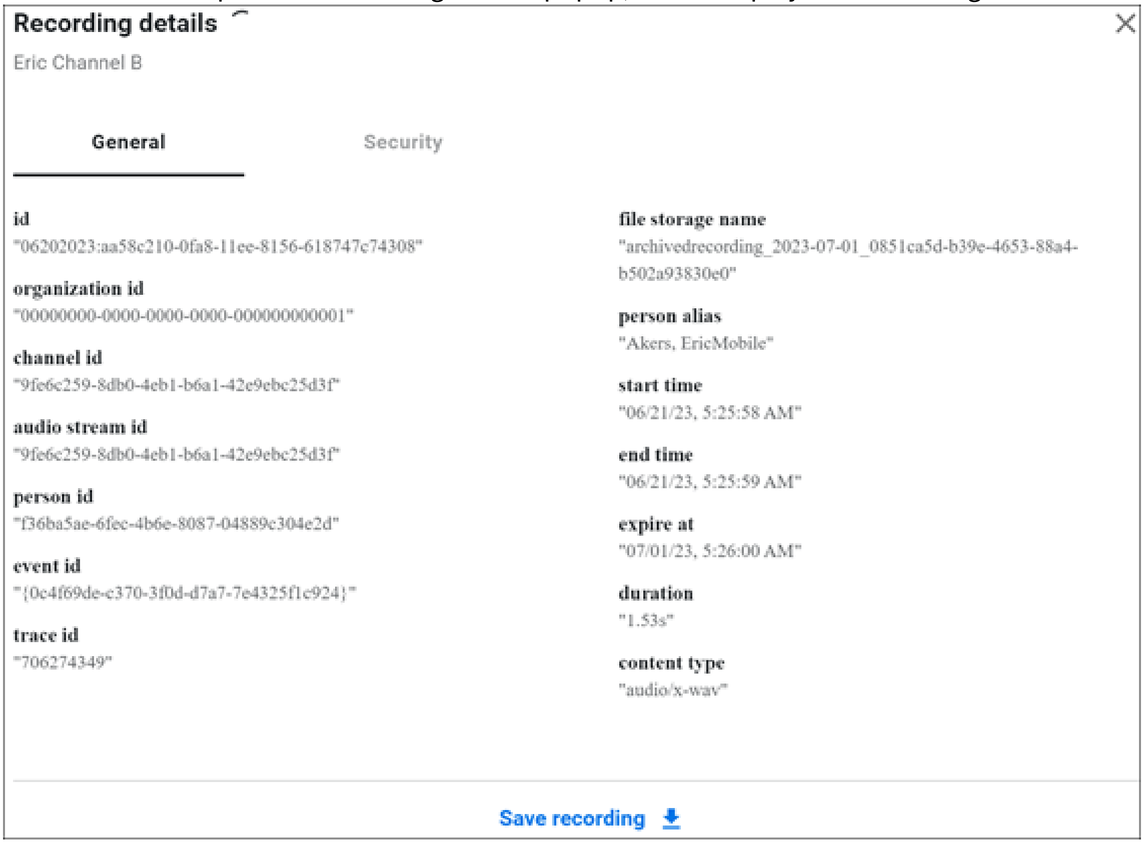
5. Select 'Recorded'. The audio activity on that channel will now be recorded. The archived recordings will be available at Settings > Archive Recordings.



9.2 Listen to a recording

1. Got to 'Settings' > 'Archived Recordings'.
2. Refine the list of recordings using the filters:
   - Channel
   - Person (user)
   - Timeframe (date and time)
3. Select to play and/or download the recording.

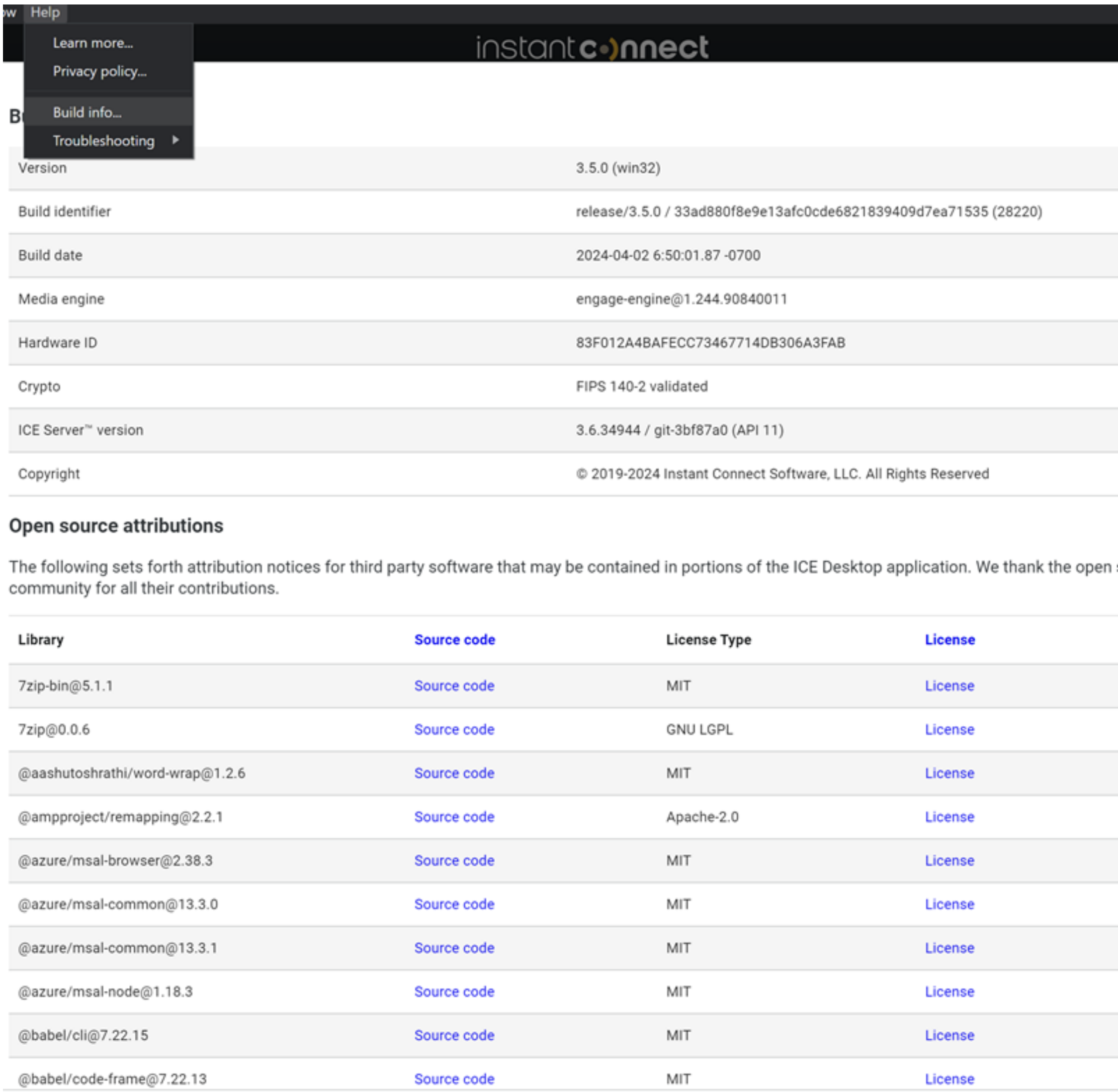
4. Select the Info icon to open the 'Recording details' popup, which displays the recording's meta-data.



10 Obtaining ICE Desktop Build Information

Build information includes information that can help our support team provide assistance with ICE Desktop.

To access build information, from the menu bar, select **Help** -> **Build Info**. The Build Info screen opens. You can cut and paste information from this screen into an email message or other document to share

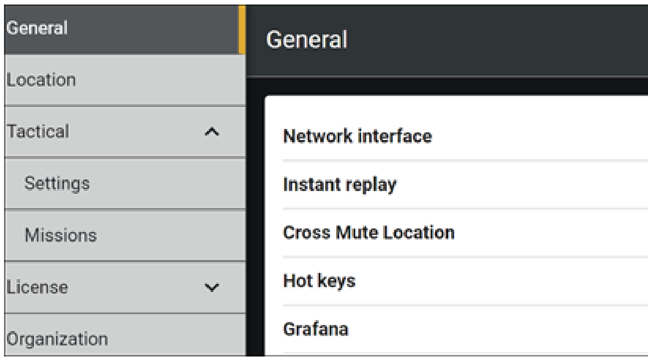


with the support team.

11 General Settings

Use the General menu to configure a variety of system settings and operations.

Access the General settings form from the Settings window select **General** menu option.

The following figure describes the options in the General menu. 

Network Interface: Provides an option for selecting the network interface to be used for voice traffic. See the "Network Interface" section

Instant Replay: Options for configuring Enable / Disable and limits for Instant Replay

Hot Keys: Provides the ability to Create and assign an Action for Hot Keys

Notifications: Enable / Disable notification when audio is received on a channel or on a incoming telephone call

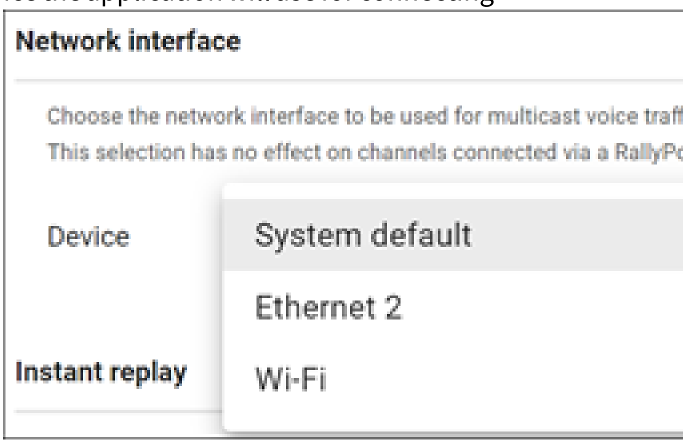
Push to Talk Sounds: Enable / Disable notification sounds and set the volume level for PTT Granted, PTT Denied, PTT End and PTT Received

Error Sounds: Enable / Disable notification sound and set the volume level for Network Channel error

Other Sounds: Enable / Disable notification sounds and set the volume level for Telephone Call and Channel Added

Crash Reporting: Option to Enable / Disable automatic reports sent on a application crash

11.1 Network Interface

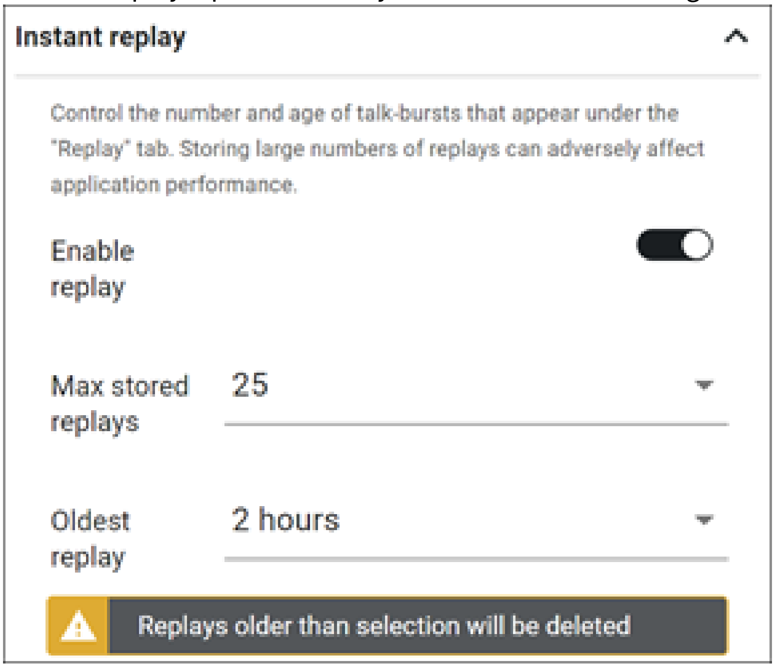
Network interface options allow you choose the network device the application will use for connecting to the network. The following table describes these options. 

Network Interface: Displays the option for choosing a network device.

Device: Selects the network interface that is used for voice communications. The operating systems default network interface card is selected by default, but it may not be the best interface to use in your situation.

11.2 Instant Replay

Instant Replay options allow you to enable and configure the limits for storing the audio files.

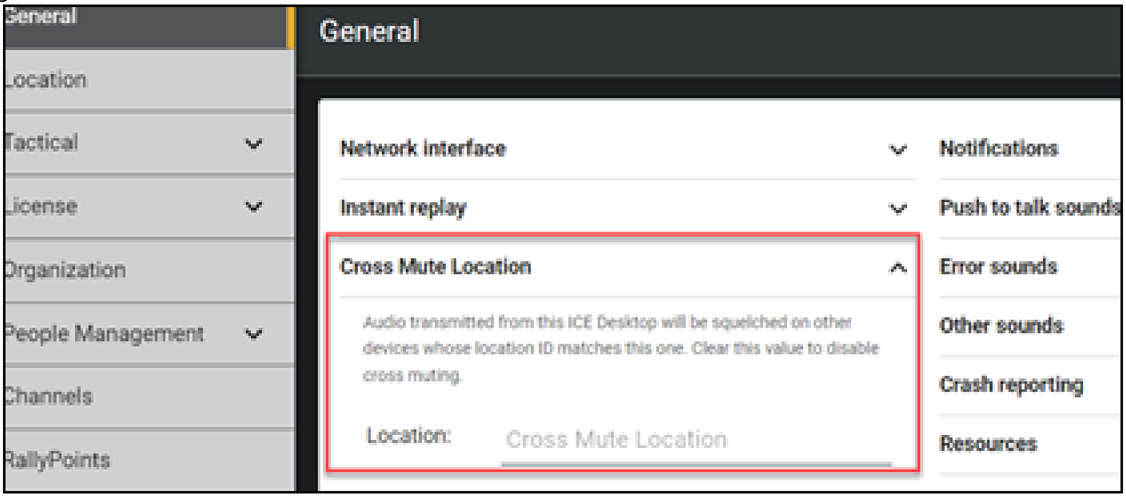


The following table describes these options.

Setting	Description
Instant Replay	Displays the options for Instant Replay settings for your client
Enable Replay	Enables or disables Instant Replay on your client. When enabled Instant Replay recordings are available for replay for the amount of time and length configured.
Max Stored Replays	Configures the maximum number of recordings to store on your client. Choose from: 25, 50, 75, 100 (Default)
Oldest Replay	Configures the length of time to archive a recording. Choose from: 24 hours (Default), 22, 20…2 hours

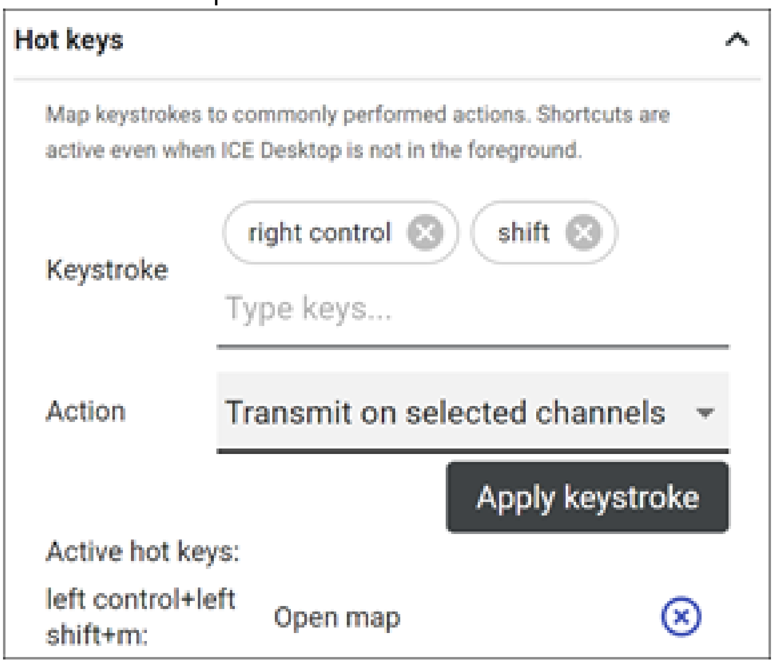
11.3 Cross Mute Location

'Cross Mute Location' allows the audio transmitted from an ICE Desktop to be squelched on other devices with matching location IDs. Enter the relevant location ID in the 'Location' field to enable. Clear the field to disable.



11.4 Hot Keys

Hot Keys allow you configure key combinations that can be used to perform common actions in the client application without having to use the mouse.



The following table describes these options.

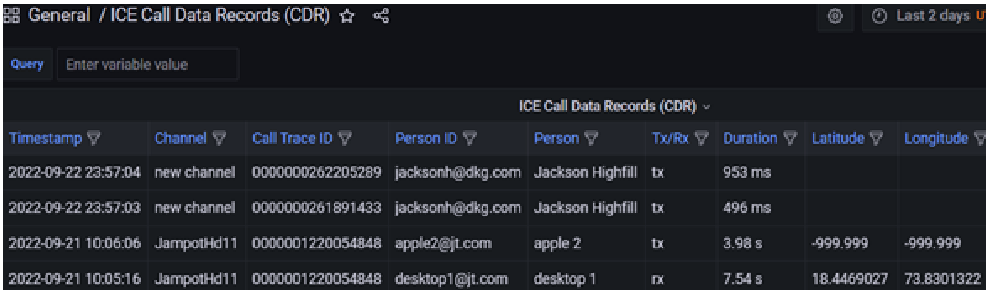
Setting	Description
Keystroke	Combination of keys used to perform the configured Action
Action	Action to be performed when the user presses the combination of keys configured in the Keystroke. Choose from: Transmit on selected channels, Open map, Accept call, End call, Transmit on a specific channel
Apply keystroke	Saves and activates the Keystroke configuration and the applied Action
Active Hot Keys	Lists the currently active Hot Key combinations and actions
X	Click the X icon next to an Active Hot Key to delete it

11.5 Grafana

Grafana, which serves as the presentation layer for Prometheus (metrics) and Loki (logs), is an open source analytics and interactive visualization web application providing charts, graphs, and alerts for the web when connected to supported data sources. Prometheus is an open source tool used for event monitoring and alerting, records real-time metrics in a time series database, with flexible queries and real-time alerting. Loki is an open source log aggregation system designed for resource efficiency and ease of operation.

11.5.1 Call Data Records (CDR)

CDR may be viewed using Grafana.



Timestamp	Channel	Call Trace ID	Person ID	Person	Tx/Rx	Duration	Latitude	Longitude
2022-09-22 23:57:04	new channel	0000000262205289	jacksonh@dkg.com	Jackson Highfill	tx	953 ms		
2022-09-22 23:57:03	new channel	0000000261891433	jacksonh@dkg.com	Jackson Highfill	tx	496 ms		
2022-09-21 10:06:06	JampotHd11	0000001220054848	apple2@jt.com	apple 2	tx	3.98 s	-999.999	-999.999
2022-09-21 10:05:16	JampotHd11	0000001220054848	desktop1@jt.com	desktop 1	rx	7.54 s	18.4469027	73.8301322

11.5.1.1 To view CDR

1. From the **General** screen, select the **Grafana** button to open Grafana within the desktop app's built-in web browser.
2. Select the **Open in Browser** button to open Grafana in an external web browser.

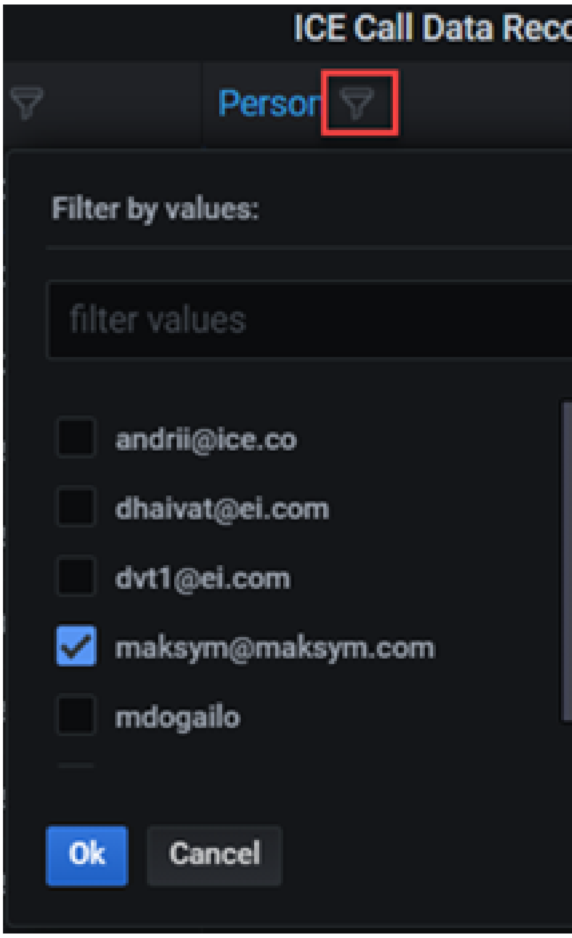
> While you *can* continue to view Grafana from within the desktop app's built-in web browser, *the external web browser view is recommended* as it makes full use of your screen, allowing for more information to be visible at once.

3. Select **Manage** from the **Dashboards** dropdown.
4. From the resulting dashboard list, select the **CDR** dashboard.

Column	Description
Timestamp	When the call occurred.
Channel	The channel on which the call occurred.
Call Trace ID	Unique system identifier for the call (a transmit and the corresponding receives).
Person ID	Unique system identifier for the user.
Person	Configured user name displayed in the UI.
Tx/Rx	The type of call activity: **tx** (transmit), **rx** (receive), **txcall** (direct call transmit), **rxcall** (direct call receive)
Duration	The duration of the call.
Latitude	The user's latitudinal location during the call.
Longitude	The user's longitudinal location during the call.
Location Age	How long ago the location data was captured, i.e, how old it is.

11.5.1.2 Sort, Query, Filter CDR

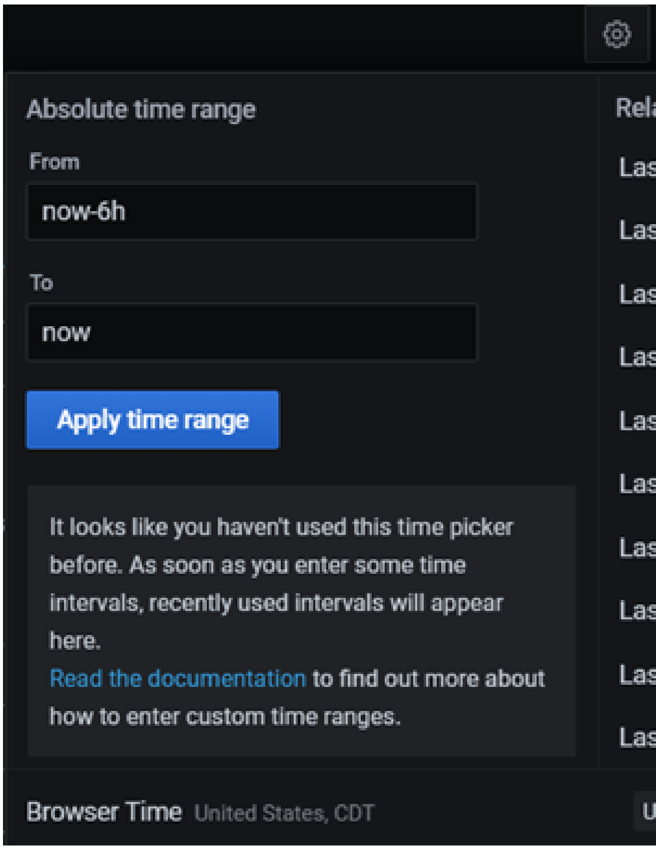
- Click on column headers to toggle between ascending/descending sorts.



- Click on column filter button to filter by selected column values.
- **Query**: Enter a value in the **Query** field, then select **Enter** on your keyboard to refine the records displayed.

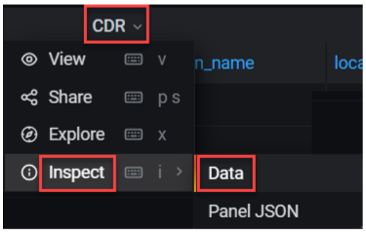
  > Tip: Triple-click on a CDR value to select it.

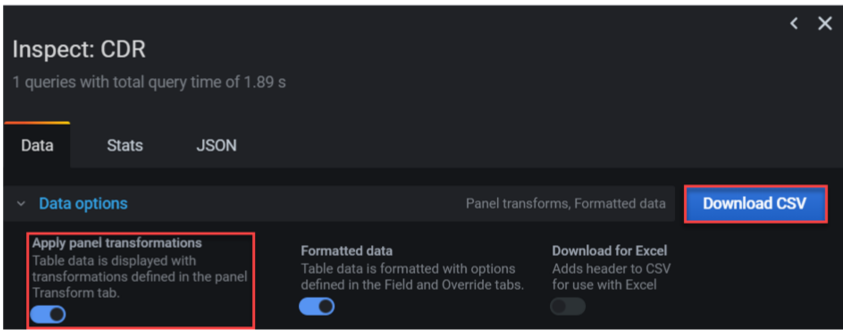
- **Time Range**: Click the **Time Range** dropdown to configure a custom time range or to select a predefined one.
- **Refresh**: Select the **Refresh** button to manually refresh the data, or select the adjacent drop-



down to configure auto refreshes at scheduled intervals.

11.5.1.3 Download CDR





11.5.1.4

1. From the **CDR** dropdown, select **Inspect**.
2. From the **Data** tab of the resulting **Inspect** screen, enable **Apply panel transformations**.
3. Select the **Download CSV** button to download the CDR dashboard data as a CSV file. The file contains the data currently displayed, reflecting any filters in effect.

11.5.2 Server Logs

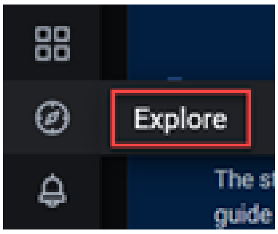
Use the following instructions to view, modify, and download server logs.

11.5.2.1 View Server Logs

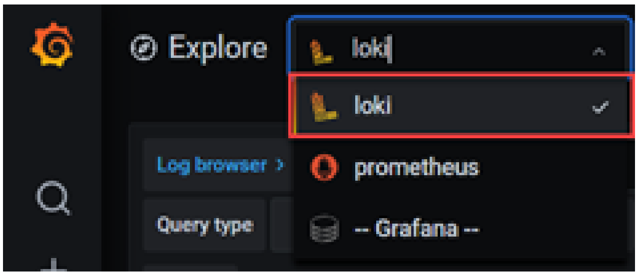
1. From the **General** screen, select the **Grafana** button to open Grafana within the desktop app's built-in web browser.
2. Select the **Open in Browser** button to open Grafana in an external web browser.

   > While you *can* continue to view Grafana from within the desktop app's built-in web browser, *the external web browser view is recommended* as it makes full use of your screen, allowing for more information to be visible at once.

3. Select **Explore** from the **Compass** icon menu.

4. From the resulting **Explore** page, make sure Loki is selected data source.

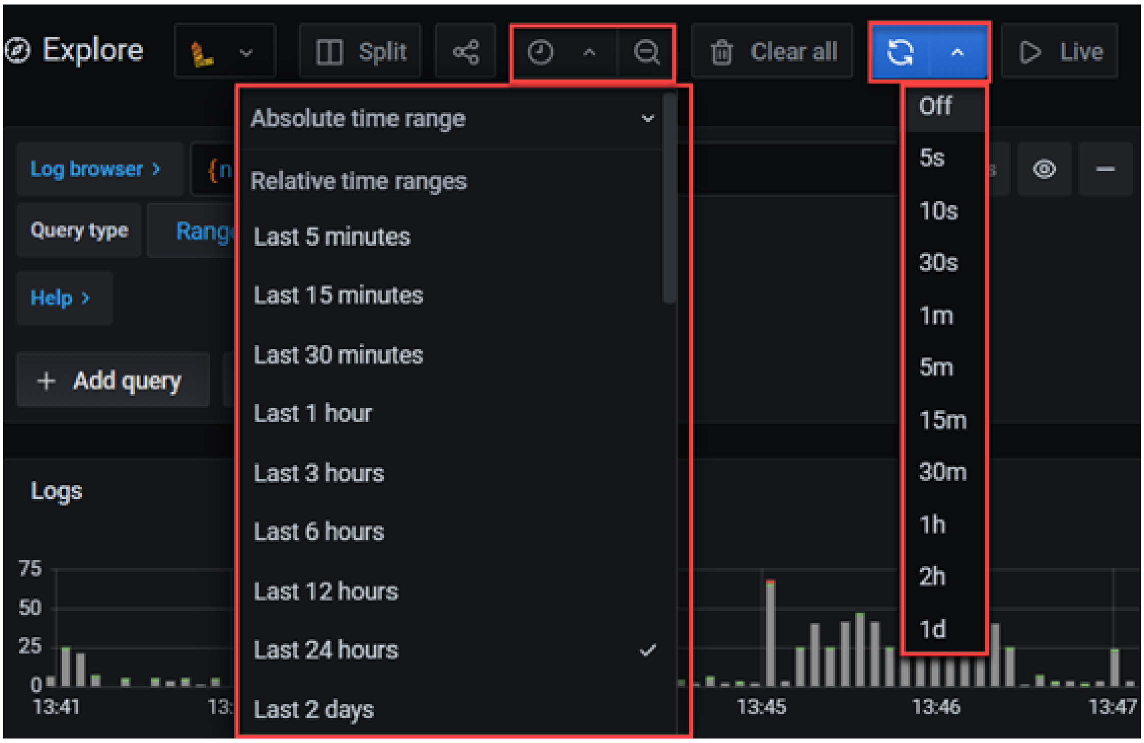
5. Select the **Log browser** button.
6. From the resulting screen, select the data label(s) and then, for each label, select the data value(s).
7. Select the **Show logs** button to view the server logs.

11.5.2.2 Interacting with Server Logs

- Select a log line to see its log details view.

- By default, the log shows 1000 log lines, this can be modified via the **Line limit** field by entering another value, e.g., 500 or 3000.

- Select the **Live** button to switch to a live feed of the server logs. In the live feed, new logs come in from the bottom of the screen and have a fading contrasting background to help keep track of what is new. Select the **Pause** button or scroll the logs view to pause the live feed and explore previous logs without interruption. Select the **Resume** button to resume the live feed. Select the **Stop** button to exit the live feed and return to the standard view.
- **Time Range**: Click the **Time Range** dropdown to configure a custom time range or to select a predefined one.
- **Refresh**: Select the **Refresh** button to manually refresh the data, or select the adjacent drop-down to configure auto refreshes at scheduled intervals.



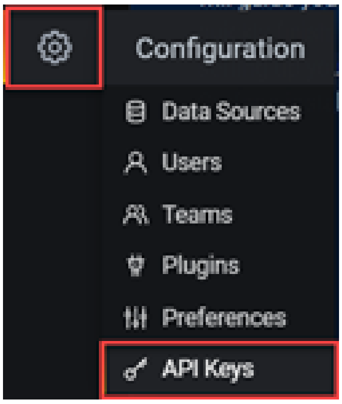
> **Note:** Above are some basic operations, for even more on exploring server logs with Grafana/Loki, please see the following Grafana documentation:
>
> - Logs in Explore

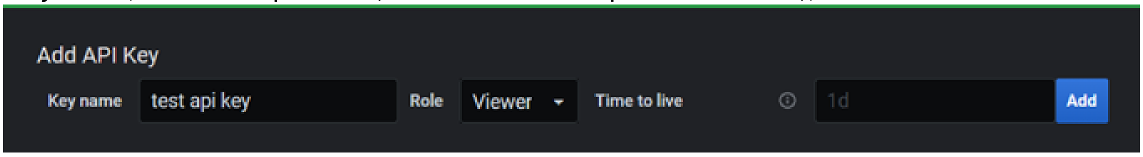
> – Using Loki in Grafana
> – LogQL: Log Query Language

11.5.2.3 Download Server Logs

1. Run the server log (see the *View Server Logs* section above).
2. Select the **Inspector** button.
3. From the resulting screen, select the **Data** tab.
4. From that tab, select the **Download CSV** button to download the serve log data as a CSV file.

11.5.2.4 APIs for Server Logs

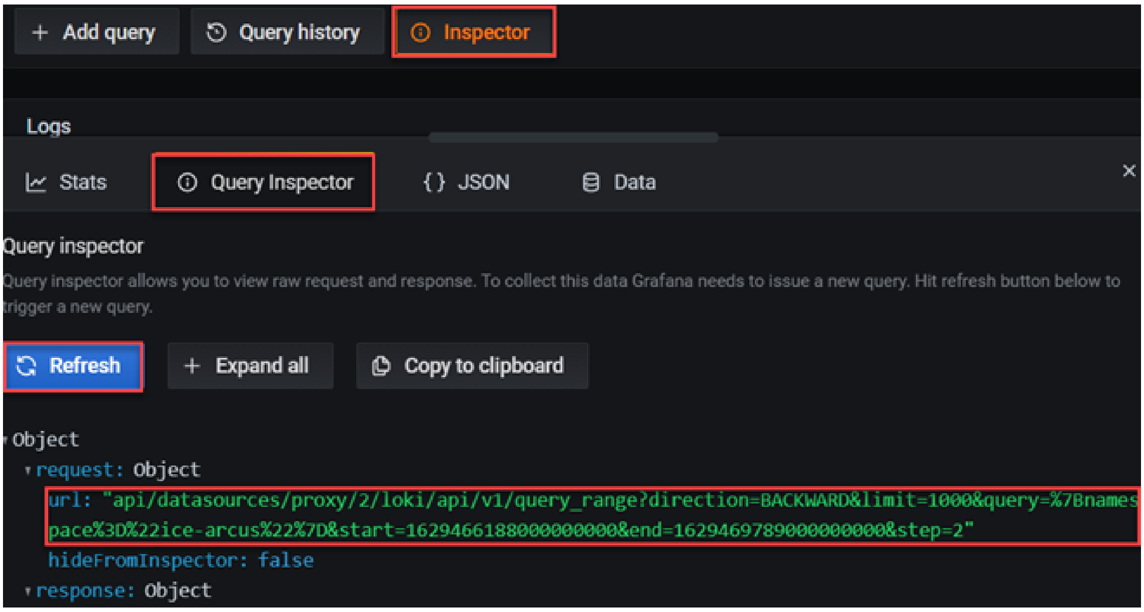
1. Get API key.
   1. From the **Configuration** (gear icon) dropdown, and select **API Keys**. 

2. From the **API Keys** tab of the **Configuration** page, select the **Add API key** button.
3. Enter the API key name, role and expiration (leave blank if no expiration desired), and select the **Add** button. 

   4. From the resulting **API Key Created** popup, ***copy the API key***.

   > **Note:** You can only view this key here this one time, so be sure to ***copy it now!***

4. Get the URL.



   1. Run the server log (see the *View Server Logs* section above).
   2. Select the **Inspector** button.
   3. From the resulting screen, select the **Query Inspector** tab.
   4. From that tab, select the **Refresh** button.
   5. Copy the URL.

5. Combine the API key and URL to create the command. The format is:

```
curl -H "Authorization: Bearer [API key]" 'https://staging.
    instantconnect
enterprise.com/grafana/[URL]
```

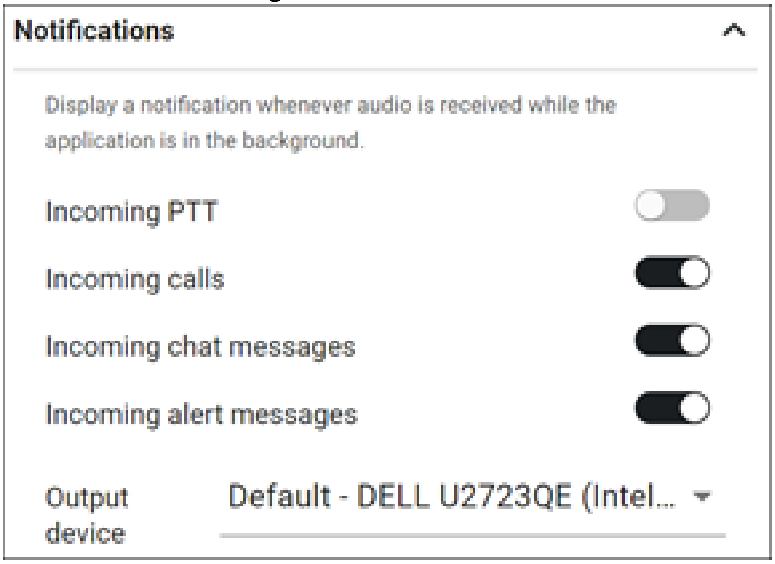
> **For example:**
>
> If the API key is:
>
> ```
> eyJrIjoiV0IwcGJ5c0Z5c040a2pDeFlDNUtGeXlDWHFZWUkyY0ciLCJuIjoibW4gdG
> VzdCIsImlkIjoxfQ
> ```
>
> and the URL is:
>
> ```
> api/datasources/proxy/2/loki/api/v1/query_range?direction=BACKWARD
>     &limit=1000&query=%7Bnamespace%3D%22ice-arcus%22%7D&start
>     =1629402190000000000&end=1629405791000000000&step=2
> ```
>
> Then the command is:
>
> ```
> curl -H "Authorization: Bearer eyJrIjoiV0IwcGJ5c0Z5c040a2pDeFlDNU
> ```

```
tGeXlDWHFZWUkyY0ciLCJuIjoibW4gdGVzdCIsImlkIjoxfQ==" 'https://
    staging.instantconnectenterprise.com/grafana/api/datasources/
    proxy/2/loki/api/v1/query_range?direction=BACKWARD&limit=1000&
    query=%7Bnamespace%3D%22ice-arcus%22%7D&start
    =1629402190000000000&end=1629405791000000000&step=2'
```

> **Note:** The URL in the example command above is encased in single quotes to prevent the terminal from trying to interpret the ? and & characters.

11.6 Notifications

Notifications are slide in messages that display whenever audio is received while in the application is in the background. A user can enable / disable the notifications with these settings.

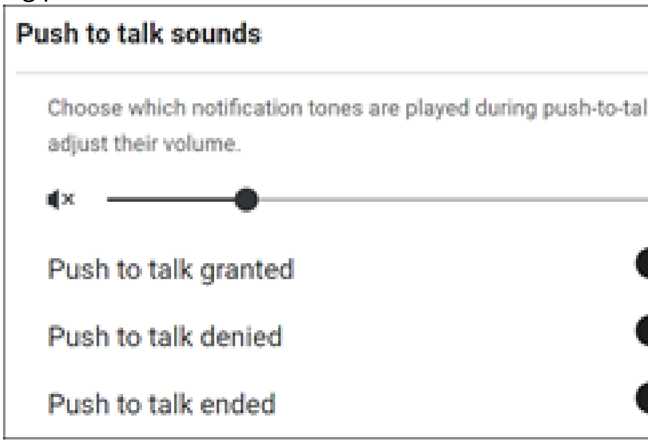


Incoming PTT: Enable / Disable notification for audio received on activated channels.

Incoming Calls: Enable / Disable notification for incoming telephone call.

11.7 Push to Talk Sounds

Push to Talk Sounds are notification tones that are played during push-to-talk events. A user can enable / disable these tones and adjust the volume of these tones.



Volume Slider: Adjust the volume of PTT notifications by sliding the level to your desired volume. Slide left to lower the volume, slide right to increase the volume.

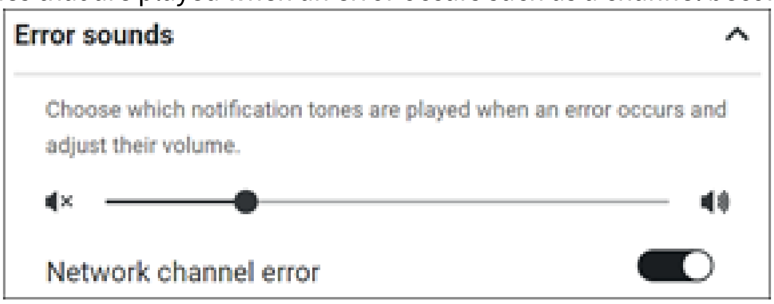
Push to Talk Granted: Enable / Disable notification tone for successful PTT button press.

Push to Talk Denied: Enable / Disable notification tone for failed PTT Grant on PTT button press.

Push to Talk Received: Enable / Disable notification tone for audio received on an active channel.

11.8 Error Sounds

Error Sounds are notification tones that are played when an error occurs such as a channel becomes disconnected from the network.

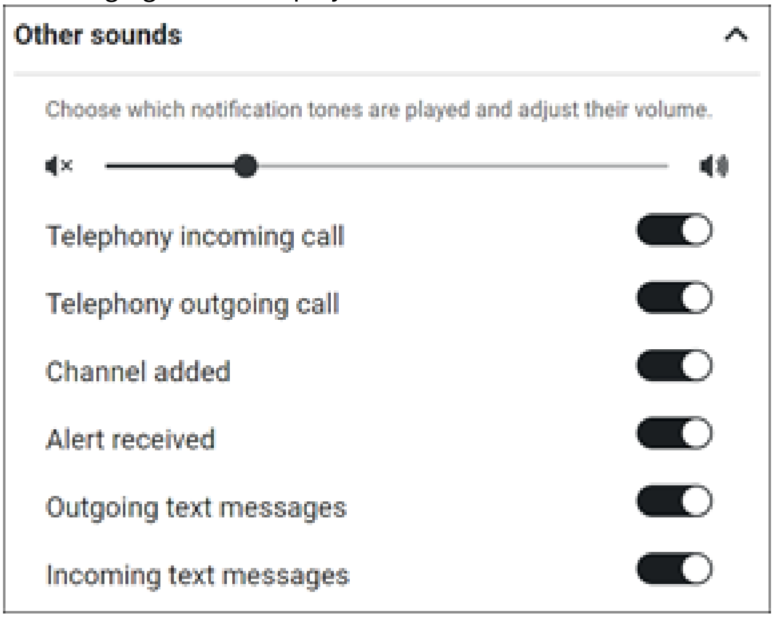


Volume Slider: Adjust the volume of error notifications by sliding the level to your desired volume. Slide left to lower the volume, slide right to increase the volume.

Network Channel Error: Enable / Disable notification tones played when a channel becomes disconnected from the network or Rallypoint.

11.9 Other Sounds

Sound notification tones for Telephone call ringing and tones played when a Channel is added to a client can be configured in this section.



Volume Slider: Adjust the volume of error notifications by sliding the level to your desired volume. Slide left to lower the volume, slide right to increase the volume.

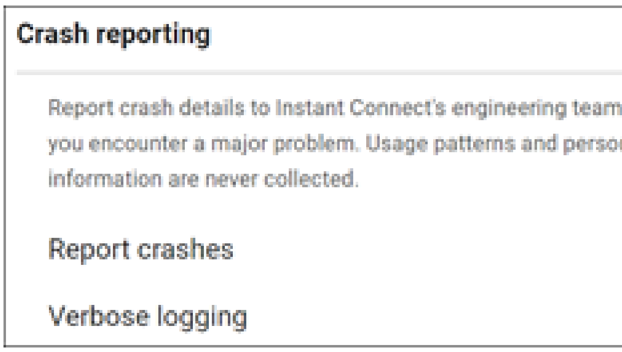
Telephone Call: Enable / Disable notification tones played when receiving or placing a telephone call.

Channel Added: Enable / Disable notification tones played when your user is added to a new Assigned or Intercom channel.

11.10 Crash Reporting

Crash Reporting when enabled allows the desktop application to report crash details to the Instant Connect Enterprise engineering team whenever the application encounters a major problem.

Usage patterns and personal information are never collected.



Report Crashes: Enable / Disable the collection and reporting of the error log files.

Verbose Logging: Enable / Disable Verbose Logging in the application. These logs contain more detail information on the operation of the application.

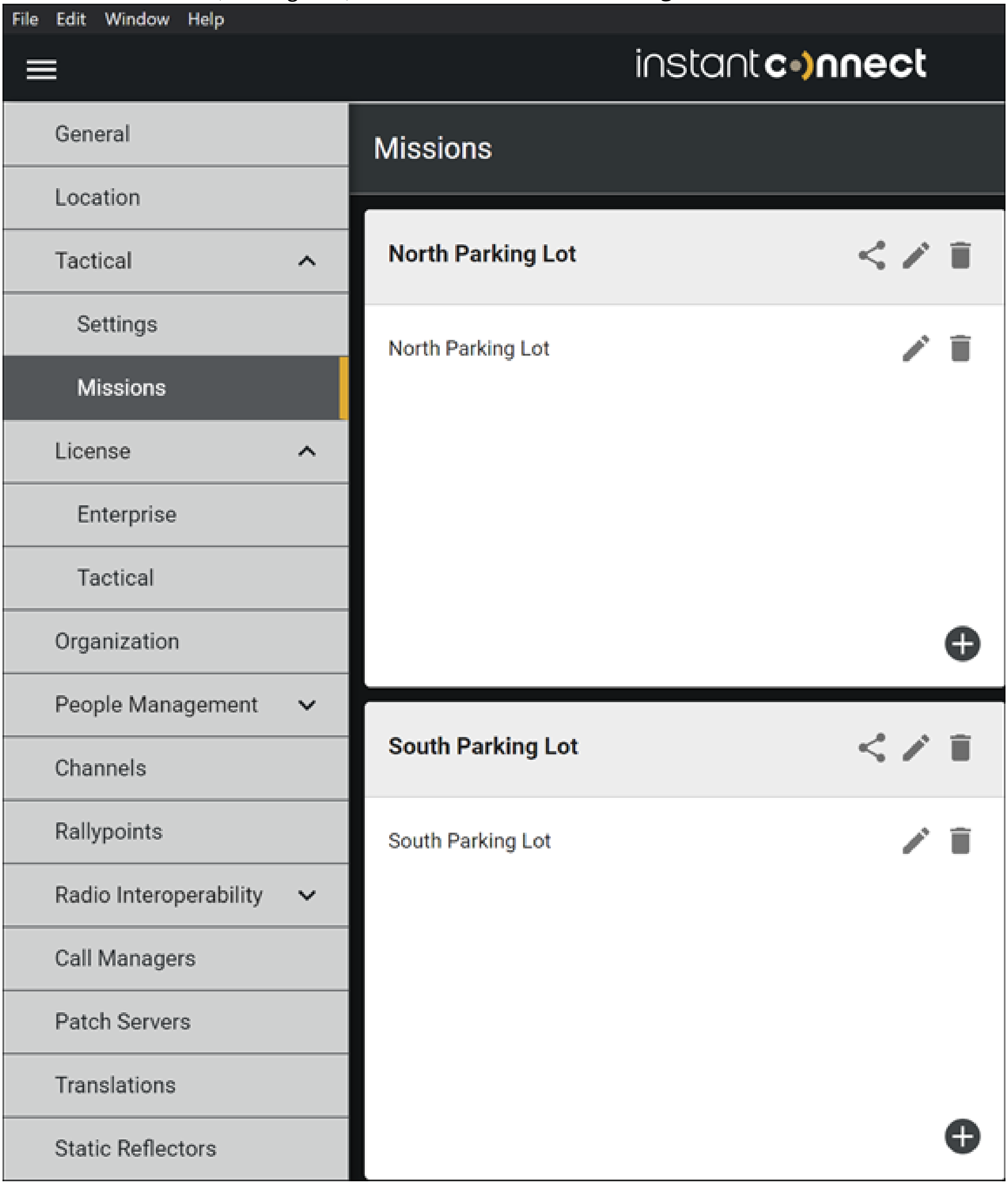
12 ICE Desktop Tactical Mode

ICE Clients have the ability run in Tactical mode, which provides the ability for the clients to operate without any server login or any connection to any server for services.

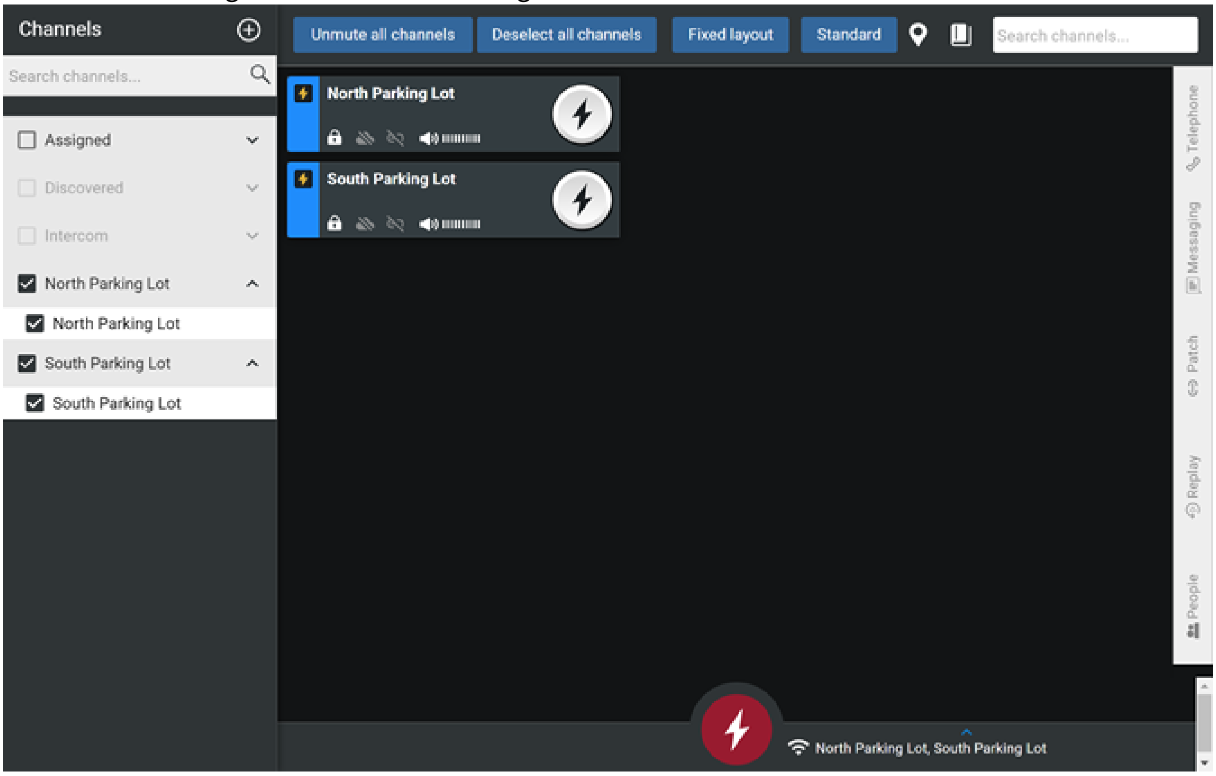
All channels are created and shared via missions that created within the application. All clients running the same mission file can communicate with each other and share user status and location information.

12.1 Viewing Missions

Missions are created, configured, and shared from the **Settings > Tactical > Missions** screen.



Active missions that are loaded into ICE Desktop are listed in the Channels list on the Channels Screen, select a mission to open the list of channels in the mission. Below the **Security Mission** is opened with North Parking Lot and South Parking Lot channels listed and active in the channels screen.

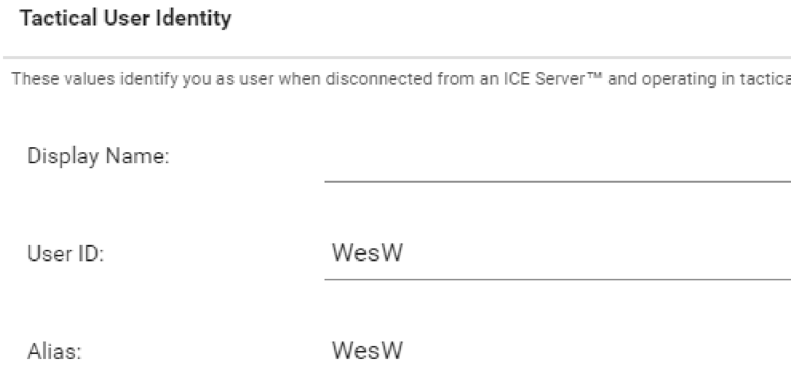


12.2 Tactical Settings

The Tactical -> Settings menu option provides the user configuration options for User Identity, License Activation and Asset Discovery.

12.3 Tactical User Identity

Tactical user identity options allow you to view and edit your identity, which is displayed to other



users. The following table describes these options.

Setting	Description
Display Name	Your full name, used to identify you in the Replay tab and User tab
User ID	Unique ID that identifies you within your organization
Alias	Alias that identifies you on radio systems or other interoperable systems

12.4 Tactical License Activation

ICE desktop client licenses can be activated and deactivated when either online or offline. Without an active license, users will find ICE features and capabilities are significantly limited, e.g., only 3 second bursts of PTT. When deactivated, licenses are returned to your organization's pool of licenses for others to use.

12.4.1 Activate a desktop license when online

1. From the desktop client, navigate to: Settings > Tactical > Settings > Tactical License Activation
2. If a Rally Tactical Systems (RTS) license:
    1. Select 'RTS License'.
    2. Enter the 'License key'.
    3. Select 'Load license file' to upload the license file.
3. If a Tactical license:
    1. Enter the 'Server Address'.
    2. Enter the 'License ID'.
    3. Select 'Load license file' to upload the license file.
4. Select 'Activate'.
5. The license is activated.

12.4.2 Deactivate a desktop license when online

1. From the desktop client, navigate to: Settings > Tactical > Settings > Tactical License Activation
2. Select 'Deactivate'.
3. For 'Are you sure you want to deactivate license?', select 'OK'.
4. The popup closes and the license is deactivated.

12.4.3 Activate a desktop license when offline

> **Note:** This process requires a mobile device, which must be online (i.e., have internet access). The ICE Mobile app does *not* need to be installed on the mobile device.

1. Start on the ***offline*** desktop:
    1. Open the ICE Desktop client and navigate to: Settings > Tactical > Settings > Tactical License Activation
    2. Enter the license key in the 'License Key' field.
    3. Select 'Offline? Activate with a mobile device'.
    4. The resulting 'Activation QR Code' popup displays a QR code. Leave this popup displayed.
2. Go to the ***online*** mobile device:
    1. Scan the QR code displayed on the desktop. It indicates a URL.
    2. Open the URL in a web browser, which leads to a webpage displaying an 'Activation Code' (it's below the QR code).
3. Go back to the ***offline*** desktop:
    1. From the the 'Activation QR Code' popup, select 'Next'.
    2. Enter the activation code.
    3. Select 'Activate'.
    4. The popup closes and the license is activated.

12.4.4 Deactivate a desktop license when offline

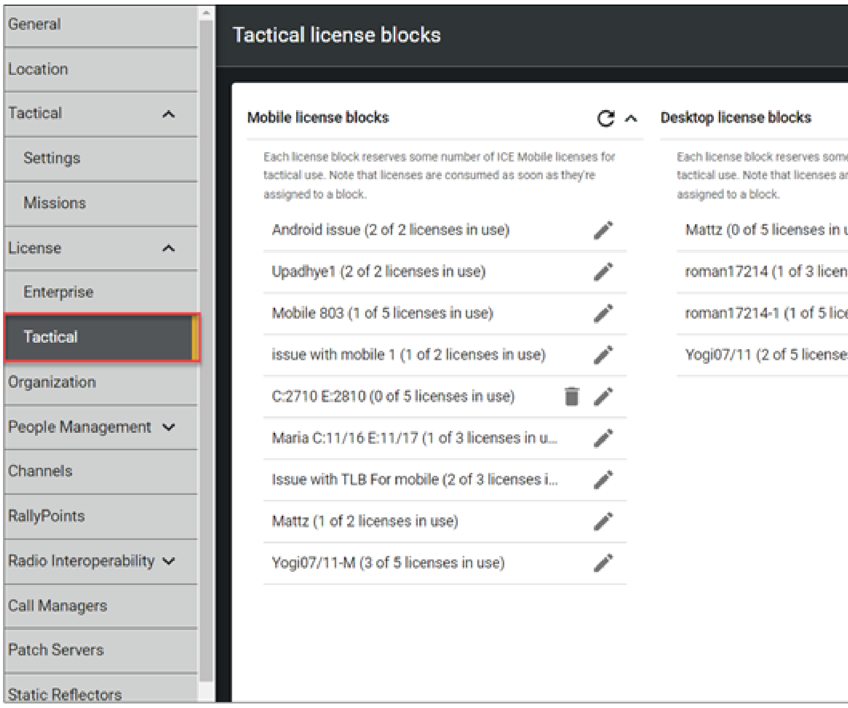
> **Note:** This process requires a mobile device, which must be online (i.e., have internet access). The ICE Mobile app does *not* need to be installed on the mobile device.

1. Start on the ***offline*** desktop:
    1. Open the ICE Desktop client and navigate to: Settings > Tactical > Settings > Tactical License Activation
    2. Select 'Offline? Deactivate with a mobile device'.
    3. For 'Are you sure you want to deactivate license?', select 'OK'.
    4. The resulting 'Deactivation QR Code' popup displays a QR code.
2. Go to the ***online*** mobile device:
    1. Scan the QR code displayed on the desktop (you may now close the popup). It indicates a URL.
    2. Open the URL in a web browser, which leads to a webpage acknowledging the license is deactivated.

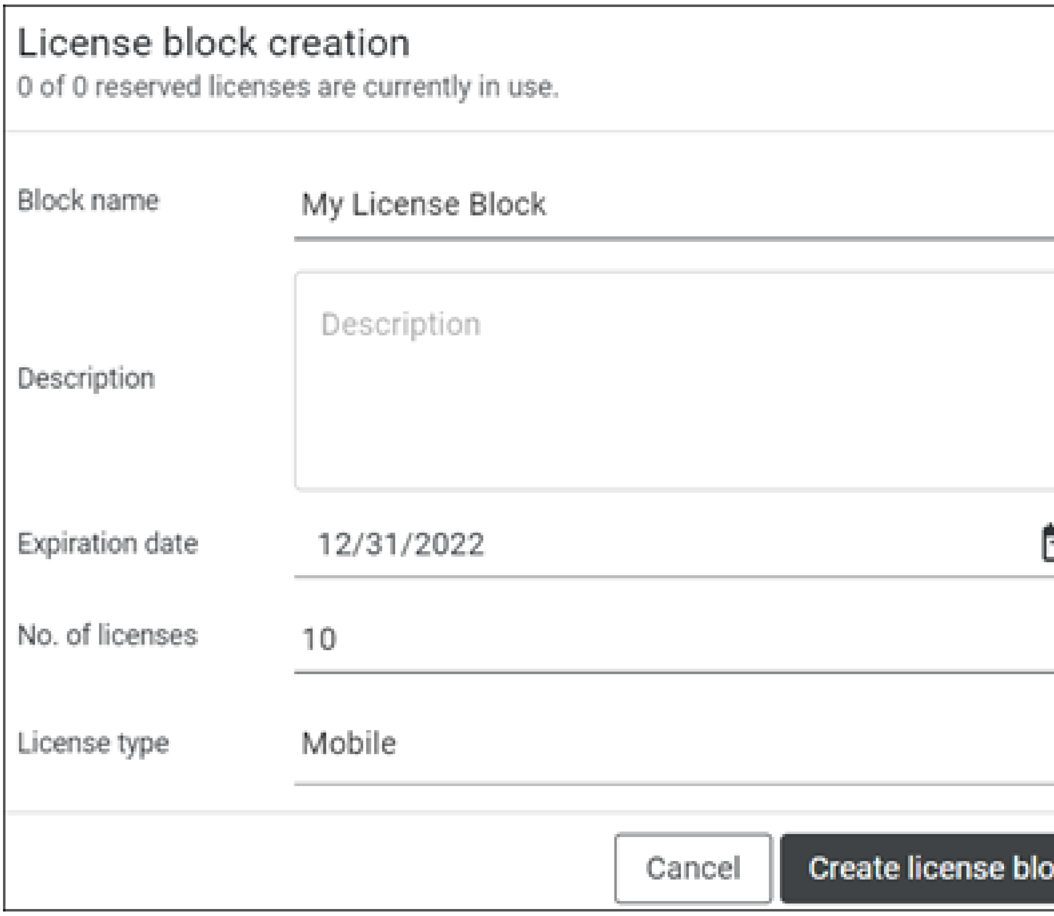
12.5 Tactical License Blocks

Organizations that have acquired a pool of tactical licenses can issue them in bulk to defined user groups. Tactical licenses, for both mobile and desktop clients, are issued with a defined duration, and on expiration are returned to the pool of available tactical licenses.

12.5.1 Create a tactical license block



1. Navigate to Settings > License > Tactical.
2. Select the + (Create license block) button in the lower, right of the screen to open the 'License



block creation' popup.

3. Populate the required fields. You can also enter additional descriptive information, if desired.

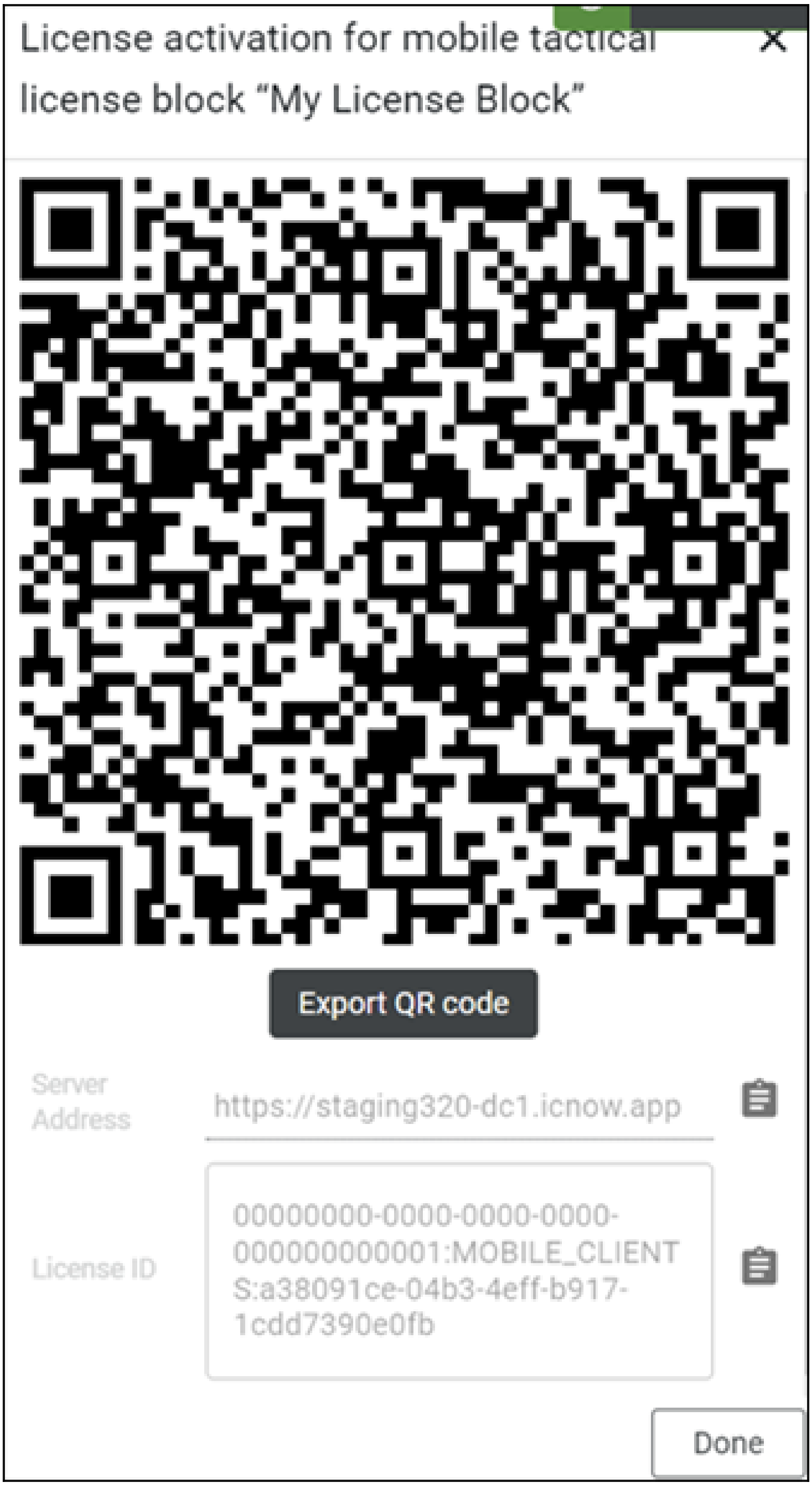
   - Block name
   - Description
   - Expiration date: The date the tactical license block expires and its licenses are returned to the pool of available licenses.
   - No. of licenses: The number of licenses in the block, which cannot be updated once the license block is created. This amount typically equals the number if users in the group, but cannot exceed the total number of licenses in the pool (minus those already reserved for other license blocks).
   - License type: Desktop or mobile.

4. Select the 'Create license block' button.

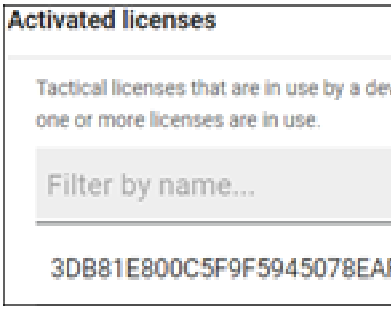
5. A banner will display confirming the new license block was created and now appears in the active license blocks list, which also indicates how many of the licenses in the block are currently activated.

6. The 'License activation' popup displays the server address and license ID used to activate one

of the tactical licenses in the block. This activation information is the same for all licenses in the block and can be shared with users via QR code (mobile only) or copied text. Select the 'Done' button to close the popup.



12.5.2 View or update a tactical license block

1. Navigate to Settings > License > Tactical.
2. Select the Edit ( ) button.
3. The license block's details are displayed:
   - Information defined by admin during creation
   - License activation information
   - List of activated licenses, including device IDs and activation dates/times: 

4. Update the license block as desired.
5. Select the 'Save' button.
6. A banner will display confirming the license block was updated.

12.5.3 Delete a tactical license block

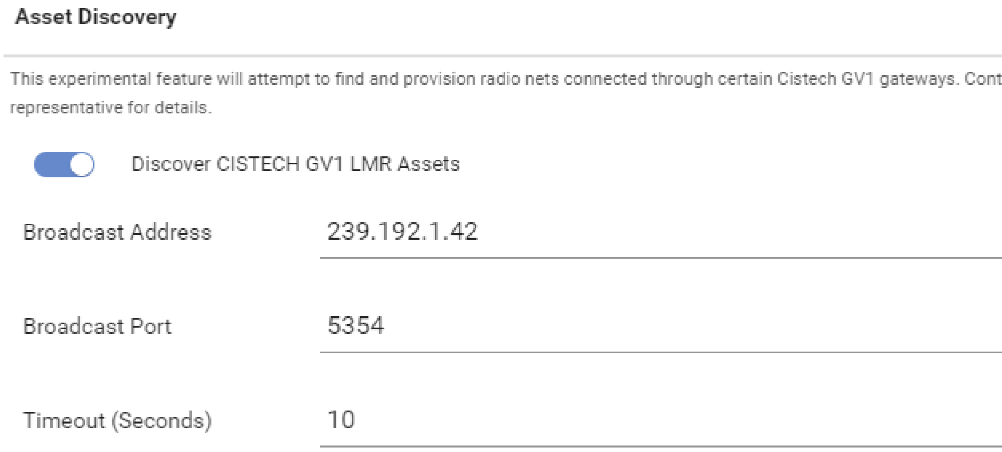
> **Note:** A license block can not be deleted if at least one of its licenses are active.

1. Navigate to Settings > License > Tactical.
2. Select the delete ( ) button.
3. Select the 'OK' button to confirm deletion.
4. A banner will display confirming the deletion.

12.6 Asset Discovery

Asset discovery options allow you to configure devices that advertise services on the network. ICE Desktop self-configures channels based on the advertisement. The following table describes these options.

Note: The asset discovery feature requires the gateway to be running a version of firmware that supports the asset discovery feature.



Setting	Description
Discover CISTECH GV1 LMR Assets	Enables or disables listening for gateway advertisements
Broadcast Address	IP address that is configured in the gateway for advertisements
Broadcast Port	IP port that is configured in the gateway for advertisements
Timeout (Seconds)	Amount of time between each advertisement of packets

13 Missions

Missions are an easy way to create and manage channels (talk groups) and participate in communication with other users across your organization from your PC. Each mission contains a group of channels that provide seamless (PTT) communication via multiple devices.

13.1 Creating Missions

You can add a mission to your ICE Desktop by creating a new mission or by importing the mission from a file from the Missions screen.

To access options for adding or importing a mission from the Missions screen click the **Plus Sign (+)**, menu options:

- **Open Mission** is used to import a mission from an file in the PC directory.

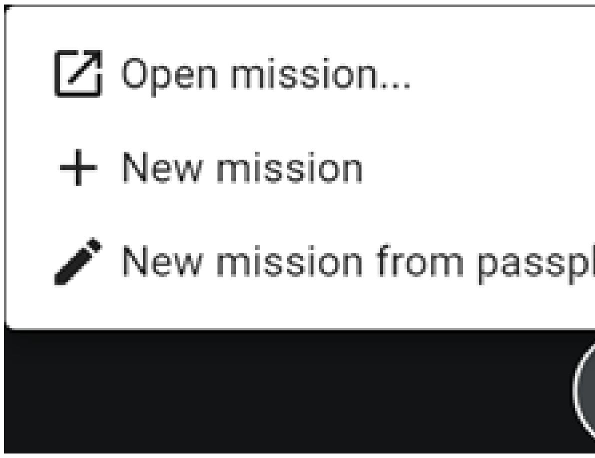
- **New Mission** is used to create a new mission that can be shared and exported to file.
- **New Mission From Passphrase** is used to create a new mission from a string of words, numbers

13.2 Create a New Mission

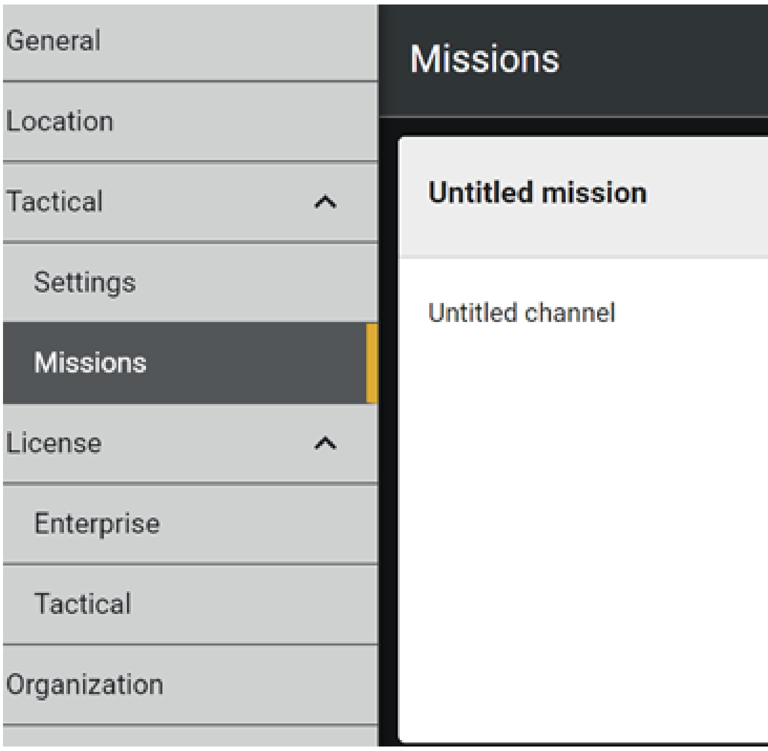
Creating a new mission file is allows the creator to share the mission file with other users that need to communicate across 1 or more channels to accomplish the task for the group. The mission file can be shared via scanning a QR code or by loading the mission file from email or directory of the client device.

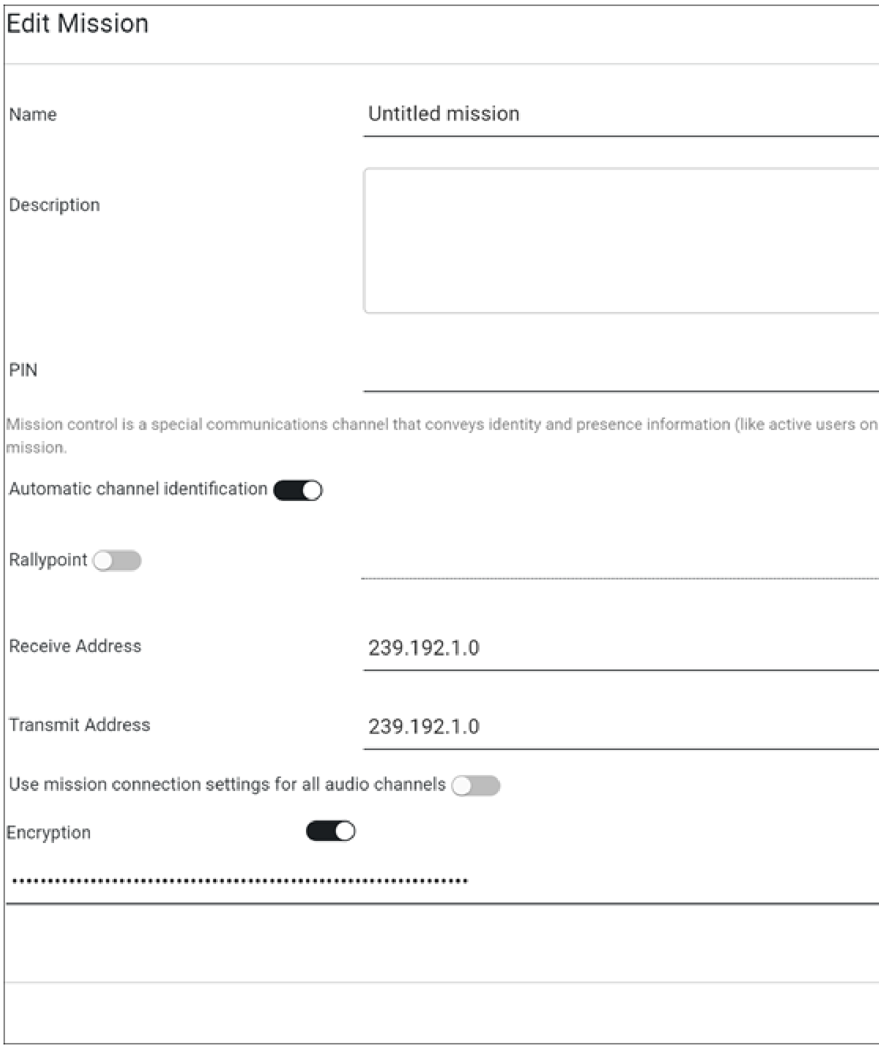
Navigate to **Settings > Tactical > Missions.**

Click the **Plus Sign** in the Missions Desktop and select **New Mission**.



A new untitled mission opens on the Missions screen.





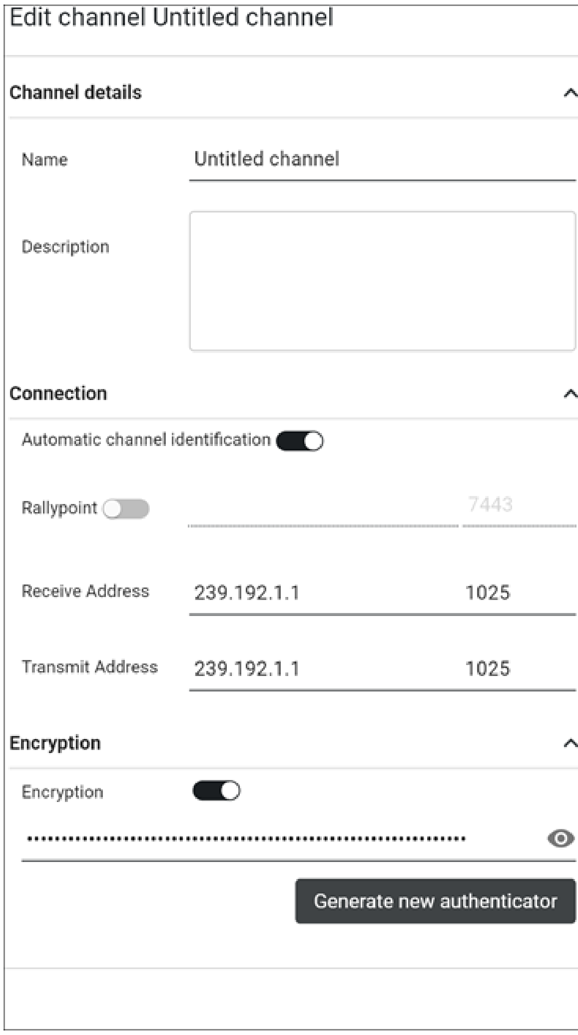
For the mission, select the Edit ( ) button.

Perform these actions in the Edit Mission box, then select ‘Save’:

Setting	Description
Name	Enter a name for the mission. The mission name does not need to be unique but it should be descriptive for users. Do not use extremely long mission or channel names if the mission file will shared via QR code. The amount of data that is allowed is a QR code is limited.
Description	In the Description field, enter a brief description of the mission.

Setting	Description
Mission Control	Mission Control is a special communications channel that conveys identity and presence information (like active users on a channel) to others engaged in the mission.
Automatic channel identification	Auto-generated unique GUID used by the system to identify this channel.
Channel ID	Manually-entered unique GUID used by the system to identify this channel.
Receive / Transmit Address	If needed, update the randomly selected IP addresses and ports that appear in the Receive Address and Transmit Address fields (3). (For information about address ranges for multicast groups, see https://en.wikipedia.org/wiki/Multicast_address-https://en.wikipedia.org/wiki/Multicast_address.)
Rallypoint	Enable and configure the use of a Rallypoint for this Mission Control channel.
Encryption	If needed, disable the Encryption option (4), which is enabled by default. Enable encryption on the mission control to ensure the data on the control will not be sent in the clear and could be compromised by a network packet capture.
Generate new authenticator	Generates an encryption key that is used to encrypt data communications on the mission control channel. Used when Encryption is enabled. Changing the encryption key without sharing the new encryption key to all other users on the mission will cause interrupted communications

For the channel, select the Edit ( ) button. In the ‘Edit channel’ screen that opens, configure the channel options for the new channel as shown in the following figure:



Channel Details

Name: Enter the name for the channel. The mission name does not need to be unique but it should be descriptive for users. Do not use extremely long mission or channel names if the mission file will shared via QR code. The amount of data that is allowed is a QR code is limited.

Connection

Automatic channel identification: System generated identifier that users use to access the channel.

Rally Point Toggle: Enables or disables the use of Rallypoint on the channel.

Receive Address: Multicast address and port on which audio is received for the channel. The transmit and the receive multicast address and port combinations can be the same, but do not need to be.

Transmit Address: Multicast address and port on which audio is transmitted for the channel. The transmit and the receive multicast address and port combinations can be the same, but do not need to be.

Encryption

Encryption Toggle: Enables or disables encryption on the channel.

Speaker

Speaker Volume: Drag the slider bar to increase or decrease the volume of this channel. Volume on other channels may be diffrent.

Speaker: Select the speaker that plays audio from the channel for the your device.

Microphone

Microphone Source: Select the microphone that you use to speak on the channel.

Advanced Settings

Header Extension Toggle: Enables or disables header extensions. When enabled, the system allows header extensions on packets to include additional data about the transmitting user.

Full Duplex Toggle: Enables or disables full duplex mode. When enabled, a party on the channel can send and receive audio at the same time.

Codec: Select the audio codec to that the channel uses.

Interoperability: Select the radio interoperability type from Default, Trellisware, Persistent Systems, Vocality, and Cistech.

Frame Size: Select the size of audio frames that are transmitted on the network.

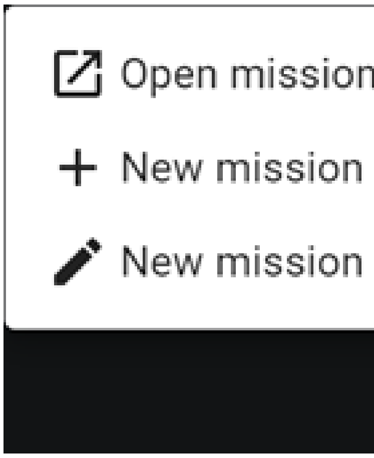
Limit Transmit: Enables or disables transmission limitations. When enabled, enter the number of seconds the that a user can transmit audio during a single PTT activity.

Alias: Enter an alias to identify users on radio system or other interoperable systems.

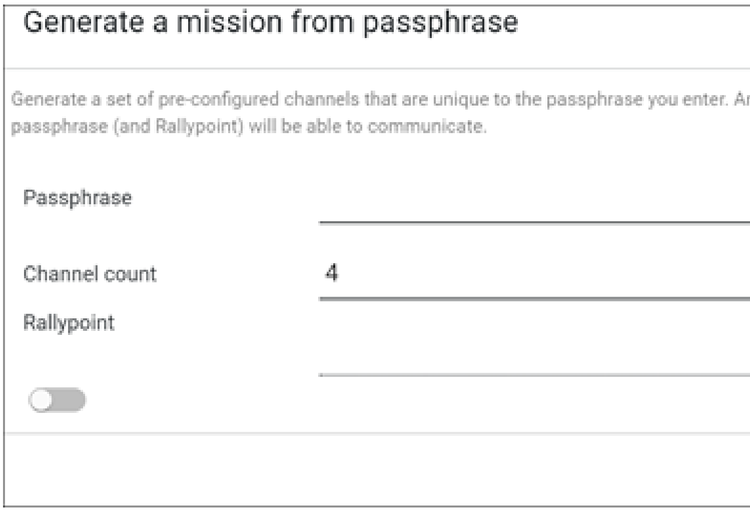
13.3 Create a New Mission From Passphrase

Creating a new mission file is allows the creator to share the mission file with other users that need to communicate across 1 or more channels to accomplish the task for the group. The mission file can be shared via scanning a QR code or by loading the mission file from email or directory of the client device.

Navigate to Settings > Tactical > Missions.



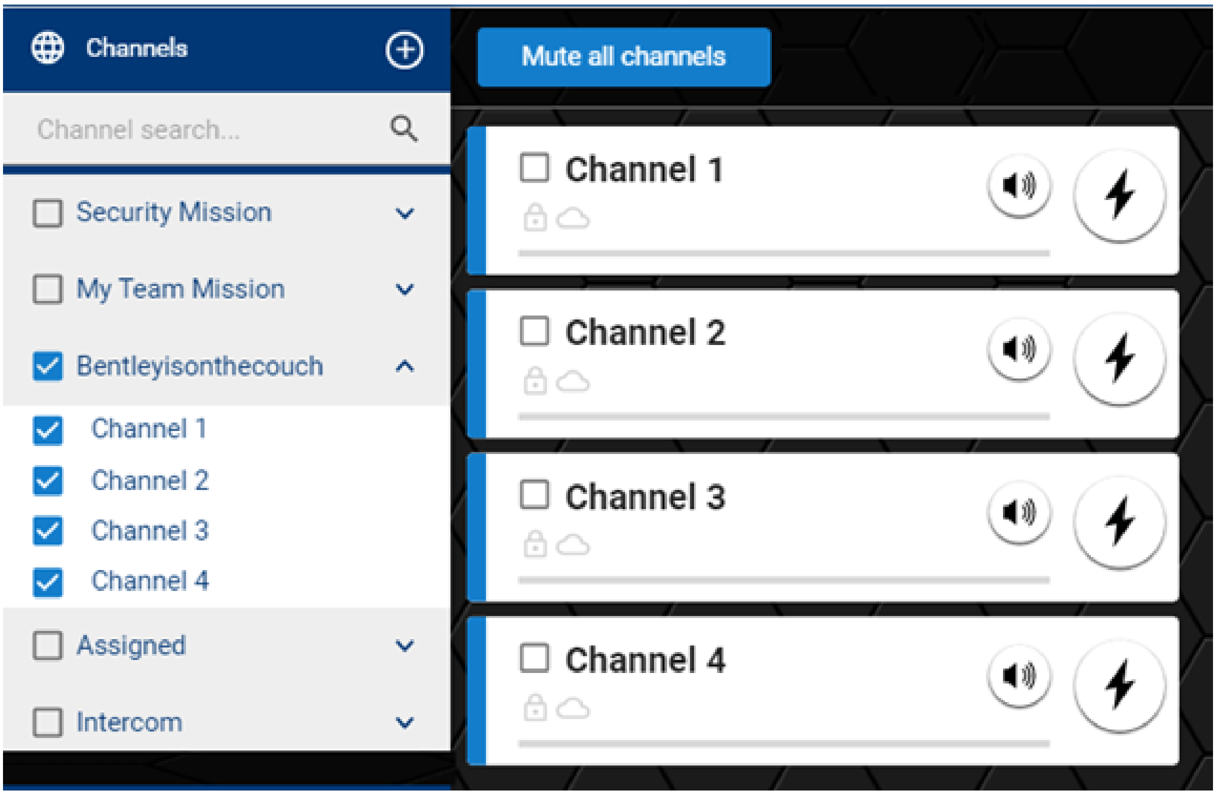
Click the **Plus Sign** in the Missions Desktop and select **New Mission From Passphrase**.



Generate a mission from passphrase form is displayed.

Setting	Description
Passphrase	Enter the Passphrase to be used to generate the unique mission. (min 15 characters)
Channel count	Enter the number of channels to be created in the mission. (1 - 25)
Rallypoint	Enable and configure the use of a Rallypoint for this mission.

The new mission is created and available in the channel list. Any other ICE client the uses the same passphrase, channel count and Rallypoint will be able to communicate with you on the channels.

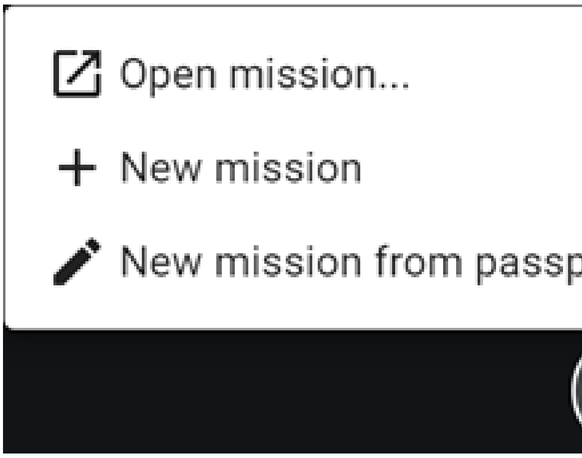


13.4 Open a Mission

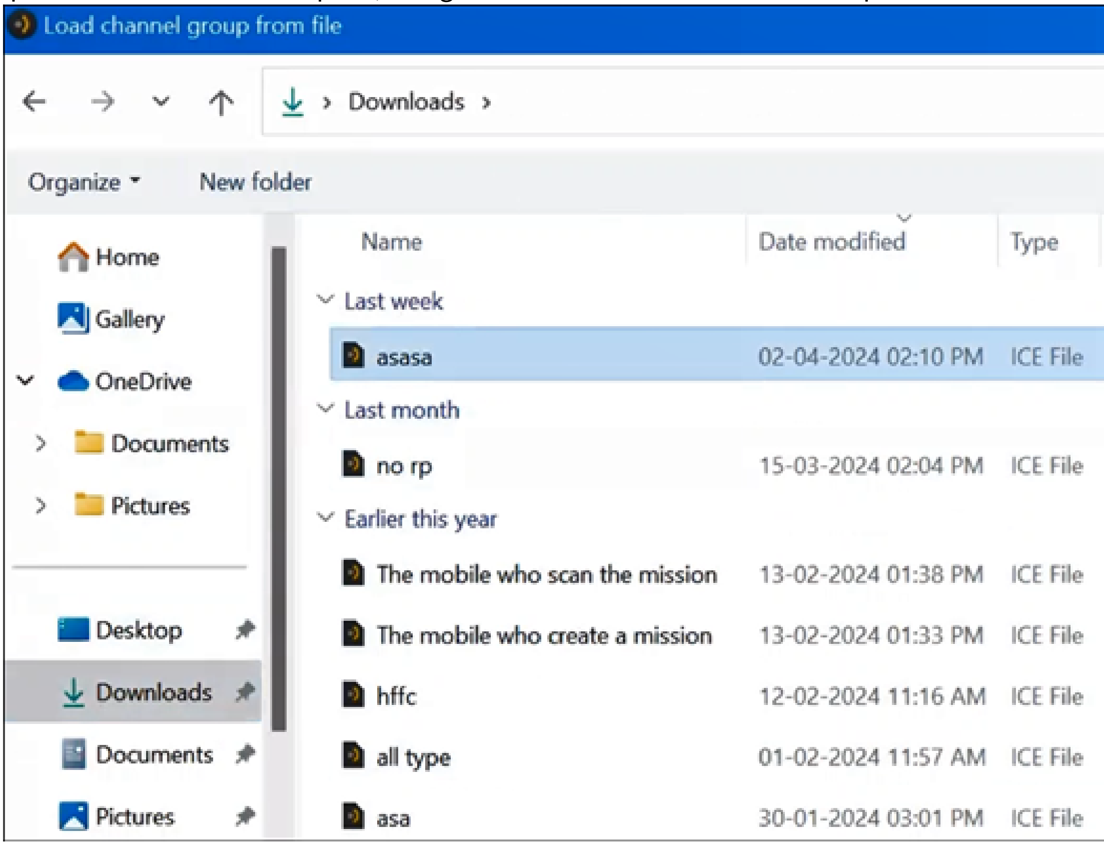
Open a Mission is used to create the channels that will used to communicate with other users on the same task force. The mission file needs to be available on the PC running the ICE Desktop application via email, USB drive, network storage etc.

Navigate to **Settings > Tactical > Missions.**

Click the **Plus Sign** in the Missions Desktop and select **Open Mission**.



In the Load Channel Group from File window that opens, navigate to and select the mission to import



and then click **Load File**.

The Mission is added to the Tactical menu and appears in the Mission desktop, just as seen in the 'Create a New Mission' section above.

> **Note:** If a mission is active on ICE Desktop, but the ICE Desktop is closed, then double-clicking on the mission's ICE file automatically opens the ICE Desktop app.

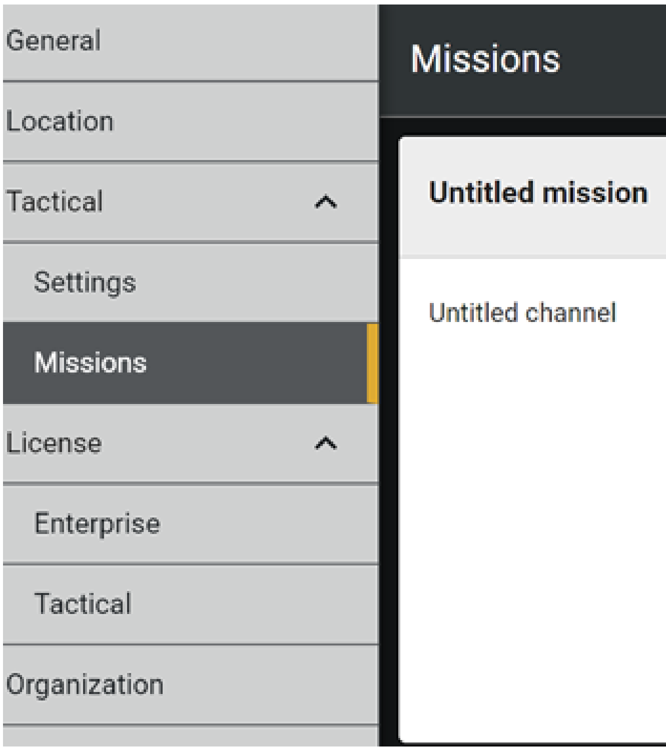
13.5 Configuring Mission Settings

You can configure a mission and channel by selecting the respective Edit ( ) button.

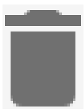
Note: Options in the Mission desktop control how your device communicates with your peers. All users who communicate on the same channels or mission should use the same configuration setting. Changes to configuration settings can prevent you from being able to talk to other users in this mission.

13.6 Adding or Deleting Mission Channels

The Channels tab provides options for adding or deleting mission channels. Any user can delete a channel from the mission. Deleting a channel from a mission will remove the channel from the users device and does not effect the channel on other users devices.



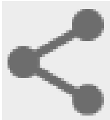
To add a mission channel, select the + button.

To delete a mission channel, select the  button.

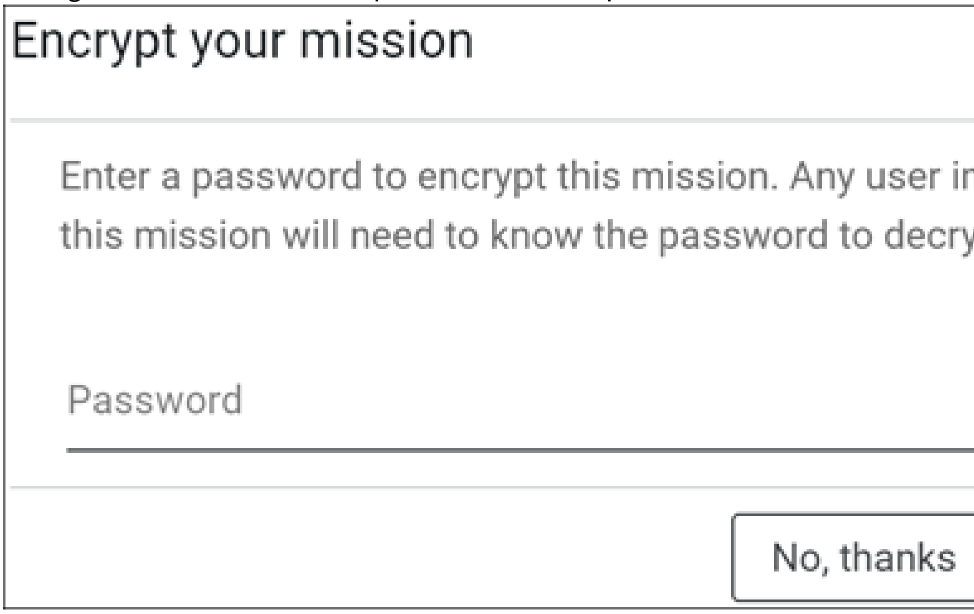
13.7 Sharing a Mission

Sharing mission file allows the creator to share the mission file with other users that need to communicate across 1 or more channels to accomplish the task assigned to the group users. The mission file can be shared via sending a QR code or by sending the mission file as an attachment in email or as a file on a USB drive.

The Share tab provides options for sharing a mission with users via a file. A mission file can be saved to the file directory of the device. The mission file can be sent to other users via email or USB file share and the other users can load the mission file on their ICE Clients to participate in the mission communications.

To share a mission, select the  button. From the resulting screen… 

…enter the URL to which a user is directed after scanning QR code, if scanned with a tool other than an Instant Connect client. A mission file QR code scanned with a ICE Client will recognize the QR code format and read the mission file ignoring the Deflection URL.

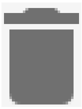
Then select **View QR code**. There is an option to encrypt the mission by entering a password. With QR code password protected a user importing the mission will need to provide the correct password in order to read and import the QR code. 

Either enter a password and select **OK**, or skip entering a password and select **No, thanks**. The QR code now displays. The QR code may be scanned directly from the screen or saved as a file that can be

shared via email, hard copy, or another method.

Alternately, instead of using a QR code, a mission can be shared via file sharing by selecting **Share file**, instead of **View QR code**. You are given the same option to enter a password for encryption. A user importing the mission will need to provide the correct password in order to import the mission. After selecting **OK** or **No, thanks**, a WindowsExplorer screen opens, allowing you to name the mission file and select a location to download it. The downloaded mission file can be shared via email, hard copy, or another method.

13.8 Deleting Missions

To delete a mission, select the  button. The mission card and channels will be removed from the ICE Desktop. The deleted mission can be imported in from the mission file again if needed.

14 Appendix A: Add firewall rule for ICE Desktop to receive audio

Depending on your organization's IT policies, some Windows 10/11 workstations may need to add a firewall rule to allow ICE Desktop to receive audio on multicast channels.

1. From the 'Start menu' or 'Settings', search for and open 'Windows Defender Firewall'.
2. From the resulting screen, select 'Allow an app or feature through the Windows Defender Firewall'.
3. Scroll down the 'Allowed apps and features' list to find and select 'ICE Desktop' or 'ice desktop.exe'.
4. Select 'Remove'. The selection no longer appears in the list of allowed apps.
5. Repeat until all instances of 'ICE Desktop' and 'ice desktop.exe' are removed.
6. Select 'Change Settings'.
7. Select 'Allow another app'.
8. From the resulting 'Add an app' screen, select 'Browse'.
9. From the resulting file explorer screen, navigate to the installed 'ICE Desktop' file. The path depends on the type of install:
    - **MSI:** C:\\Program Files\Instant Connect
    - **EXE (Everyone):** C:\\Program Files\Instant Connect
    - **EXE (Only me (local user)):** C:\\Users\<username>\AppData\Local\Programs\Instant Connect
10. Select the 'ICE Desktop' file.
11. Select 'Open'.

12. From the resulting ‘Add an app’ screen, select ‘Add’.
13. From the resulting screen, scroll down the ‘Allowed apps and features’ list to see ‘ICE Desktop’ appears.
14. Select ‘OK’.
15. Close ‘Windows Defender Firewall’.