FirstNet Push-to-Talk administrator guide

December 2022

December 5, 2022

Contents

Overview

FirstNet Push-to-Talk (PTT) service provides instant communication between users within a public safety organization at the push of a button. As a PTT administrator, you use the FirstNet PTT Admin Tool to manage the service. In the tool, you can create users and talkgroups, administer licenses, and more.

Get started

Review this section for a brief overview of FirstNet PTT. You can find detailed instructions in subsequent chapters. The 2 key things to review are:

- Who performs the tasks required to manage the FirstNet PTT service?
- What are the key steps they need to perform?

About FirstNet Push-to-Talk roles

Organizations in FirstNet have 1 or more administrators who create and manage profiles for their users. The organization administrators add 1 of 3 roles to FirstNet PTT user profiles.

FirstNet PTT has 2 role categories based on what the user can access: Administrator access and application access roles.

Administrator access

- **PTT administrator**—Manages PTT users and groups. This is your role. To access the mobile service, you also need the Mobile user role. Ask your organization administrator to add the role to your profile.

Application access

- **Mobile user**—Can access and use the FirstNet PTT mobile service.
- **Dispatcher**—Can access the FirstNet dispatch console. Dispatchers automatically have access to the mobile service.

For more information about other FirstNet user roles, on the user management **Help** page, read the About user roles guide.

Assign FirstNet Push-to-Talk roles in bulk

If your member profiles already exist and you want to add push-to-talk user roles, the organization administrator can upload a list of multiple users at one time.

You'll need to upload an Excel spreadsheet with the following information:

- Email address
- Last name
- First name

Resend the user activation email

As soon as the organization administrator creates profiles, we'll send users automatically receive an email with instructions to complete their activation.

Until they complete their activation, users are in Pending status on the User Management page and, while you can see them in the FirstNet PTT Admin Tool, you won't be able to manage them.

Typically, users who don't complete their activation in 1 browser session or who unsubscribe from FirstNet marketing emails will need the organization administrator to resend the activation email.

Access the FirstNet PTT Admin Tool

To access the FirstNet PTT Admin Tool:

- Log in to FirstNet and click Manage FirstNet PTT users & groups. The Admin Tool dashboard appears. For more information about the dashboard and menus, see About the dashboard.

We recommend using 1 of these browsers:

- Microsoft® Internet Explorer® 10 or later
- Mozilla® Firefox® 8 or later
- Google Chrome™ 15 or later
- Microsoft Edge® 17 or later
- Safari® 11 or later

Your experience with the FirstNet PTT Admin Tool may be affected by internet security software or firewalls. If you have issues, check your computer's internet security settings.

Log in to the PTT Admin Tool for the first time

If you're the first administrator to log in to the PTT Admin Tool, the system registers you as a super administrator. You can manage the entire organization in the PTT Admin Tool and you can assign other super administrators.

Until you or another super administrator assigns roles, other administrators are designated as unassigned and can't manage the organization, agencies, or subagencies. See Manage agencies and users.

Configure organization settings

If you're the first administrator to log in, when you do, the **Edit Entity Settings** window appears. If you're not, there's no action required.

You can opt in or out of mutual aid and mutual control participation, and edit your organization's emergency call behavior.

Note: If you opt your organization out of mutual aid or mutual control, agency administrators won't be able to turn on the emergency functions for their agency or sub agency. You can opt in at any time from the **Edit Entity Settings** window.

After you choose your organization's settings, click **Save** to go to the dashboard.

Establish FirstNet Push-to-Talk service

You set up FirstNet PTT user profiles in the **Manage users** section of FirstNet Central and then manage the service in the FirstNet PTT Admin Tool, where you can set up PTT profiles for users, send mutual aid requests and mutual control requests, manage administrators and permissions, and more.

For information about setting up LMR Interop, see Manage Land Mobile Radio (LMR) and Radio over IP (RoIP) interoperability.

Set up FirstNet PTT service

The organization administrator (or person authorized to submit orders) purchases FirstNet PTT services or licenses through their organization's FirstNet sales representative.

1. If you're not an organization administrator, skip to step 3. If you are an administrator, from FirstNet Central, click **Manage users.**
2. From the **User management** page, create FirstNet IDs for each organization member and assign push-to-talk user roles. For detailed instructions, in the User management **Help** page, read the Create and manage user profiles guide. We'll send an activation email to each user with instructions about how to activate their profiles.
3. From FirstNet Central, click **Manage FirstNet PTT users & groups.**
4. Do these things:
   - Create agencies and subagencies with PTT users
   - Assign PTT agency administrators to subagencies as necessary
   - Review the FirstNet PTT users and available licenses

- Assign licenses to each PTT user
- Create talkgroups from licensed users
- Create contact lists (optional)
- Create profile templates (optional)

As soon as you create talkgroups and contacts, they're pushed wirelessly to the agency's devices so the users can make PTT calls.

Supported devices

FirstNet Push-to-Talk is supported on a variety of Android® and Apple® devices. Some devices come with FirstNet PTT embedded in the operating system and offer optimized performance for FirstNet PTT.

For other certified devices, you can download the FirstNet PTT application from Google Play® or the App Store®. Find the FirstNet PTT application on the home screen of your device. If you don't see it, download the app and follow the installation instructions.

FirstNet PTT can be used only on FirstNet certified devices. To find a list of devices certified for FirstNet PTT, go to firstnet.com/FirstNetPTT/devices.

About the dashboard

Use the dashboard to view your license status, a summary of the entities you manage, and your pending and approved mutual aid requests. From the dashboard, you can access pages to manage talkgroups, agencies, licenses, contact lists, profiles, and more.

View licenses
View your organization summary
View and manage mutual aid and mutual control requests
View alert notifications

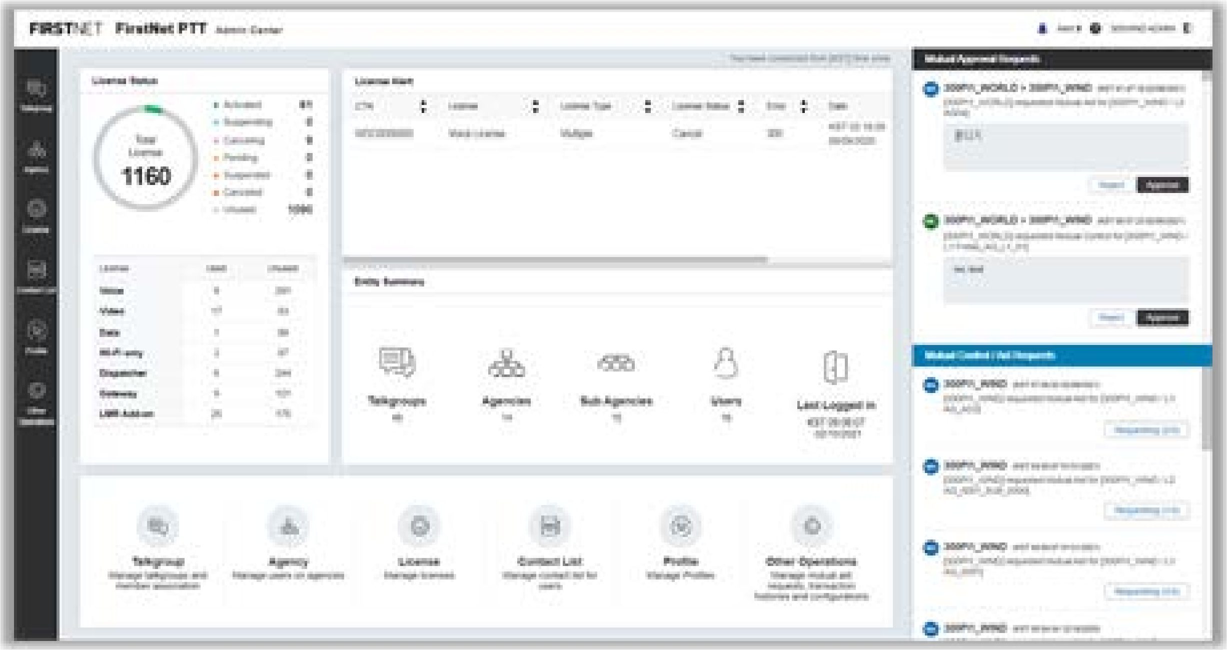


Figure 1: PTT Admin Tool dashboard

View licenses

You can view license status and alerts.

View license status

1. Open the PTT Admin Tool.

2. In the license status chart, view the following statistics of each license status:
   - Number of total licenses
   - Number of activated, suspending, canceling, pending, suspended, and canceled licenses
   - Number of unused licenses
3. To see more details about your license status, click Total License in the circle showing your license count.

For more information about managing licenses, see Manage push-to-talk licenses.

View license alerts

The License alert section shows status notifications if a license is canceled, suspended, or otherwise modified. Current license alerts are shown in this table:

Item	Description
License	Voice user Video license Video user Data user Data license LMR add-on user LMR Interop add-on license
License status	Current license status (cancel, suspend, modify)
Error	Number of license errors
Date	Date and time the error occured

Table 1: License alerts

View your organization summary

The **Entity Summary** section provides an overview of the FirstNet PTT service that you're responsible for. This section shows the following information:

- Talkgroups
- Agencies
- Subagencies
- Users
- Date and time of last login

View and manage mutual aid and mutual control requests

To manage the inter-agency requests you've submitted and received, use the **Mutual/Approved Requests** and **Mutual Control/Aid Request** sections on the right side of the dashboard.

For more information on mutual aid requests, see Manage mutual aid requests.

Approve or reject incoming mutual aid requests

1. In the **Mutual/Approved Requests** section, find the request, and click **Approve** or **Reject**.
2. To finish approving requests, select the users you want and click **OK**.

View your submitted mutual aid requests

You can find the list of your submitted mutual aid requests on the right side of the dashboard.

1. In the **Mutual/Approved Requests** section, under the request you want to view, click **Requesting (#/#)**.
2. View the status of the mutual aid request in the **Status** column of the **Mutual Aid Request Status** window.

View the Requesting History page status

When you've approved or rejected some, but not all, users in a request, you can't cancel the request. The approved users can be returned to the requester.

If you click Cancel on the Requesting History page, it cancels the entire request. If some users are approved, only the approved users can be returned to the requester or revoked.

View the Incoming History page status

You can approve all or some of the requested users you manage. Each administrator can approve the same request 1 time only. You can't partially reject the selected users. You can only reject all of the users at once.

View alert notifications

You can find alert notifications on the top right corner of your dashboard. These notifications provide details about user licensing and talkgroup issues that may need your attention. The number of alerts is listed.

To view notifications:

- On the top right corner of the dashboard, click the Notification icon.

Manage agencies and users

Use the **Agency** page to view, add, edit, and delete agencies, subagencies, and agency users. Review your organization’s hierarchy when you’re managing agencies.

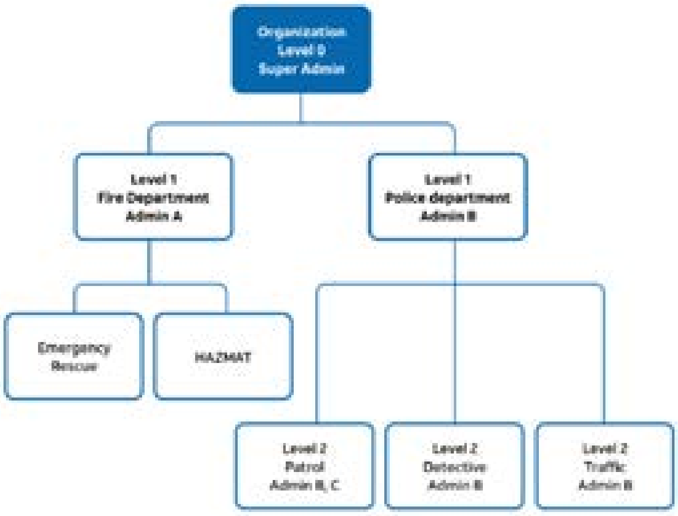
The name of your organization appears on the Agency page along with your organization ID. The organization name is the top-level name that comes from your organization’s initial setup in FirstNet. The name can’t be edited.

Understand hierarchies

Agencies can have 10 levels in the hierarchy: the organization or level 0 (organization level), level 1, and agency/subagency levels 2 - 9.

You need to define the agency organization in the system for these things:

- Organizing users in the system
- Defining administrator span of control
- Handling mutual aid & mutual control
- Setting up agency default profile (ADP)



Create and manage your organization’s hierarchies

Set up agencies and subagencies in the FirstNet PTT Admin Tool to match the existing structure of your organization.

The top level of the hierarchy is level 0, the organization itself, and is usually a public safety organization such as a city or municipality. Level 1 agencies under the organization are usually departments such as police, emergency rescue/fire, and public works.

You can establish agencies and subagencies under your organization. It can have up to 9 levels of subagencies under each level 1 agency. For example, the City of Springfield may have 3 city-level agencies: police, fire, and sanitation. The police agency may then have 2 subagencies: uniform and undercover.

Manage agencies

Use the Agency page to view, add, edit, and delete agencies.

View an agency

You can view and access only your assigned level 1 agencies and their subagencies.

1. On the dashboard, click the Agency icon.
2. From the list on the left, select the agency you want to view. A list of users appears in the table on the right.
3. The license bar at the top of the page shows the number of assigned users in the selected agency for each license type.
4. To show or hide the assigned users in the selected agency for each license type, click the License icon. To show a description of the agency, hover over the agency name and then hover over the Question mark icon that appears.

Create a subagency (Level 2 - 9)

You can create subagencies only from your assigned level 1 agencies.

1. On the Agency page, from the agency list, hover over the name of the level 1 agency you want to create a subagency under, and then click the Plus icon that appears. The **Create Subagency window** opens.
2. Select a parent agency from the list.
3. Enter a subagency name using these guidelines:
   - Use letters, numbers, and these special characters: [+ @ # $ & ( ) _ , . !]
   - If you use spaces, use only in the middle of the name, not as the first or last character
   - Use a maximum of 80 characters

4. To check for any duplicate names, click **Check.**
5. For **Mutual Control Participation** and **Mutual Aid Participation**, select **Opt-in** or **Opt-out**. You can opt in for an entire agency or for individual subagencies.
6. Provide a description up to 200 characters (optional).
7. Click **Create.**
8. In the confirmation window, click **OK.** The subagency you created appears in the agency list and the agency tree.

Edit a subagency (level 2 - 9)

1. On the Agency page, from the list on the left, click the Edit icon next to the subagency you want to edit.
2. You can edit the parent agency, the agency name, the mutual control and mutual aid participation, and the description.
3. To change the subagency's parent agency, select a different agency from the list.

   Note: If you change the parent agency, the subagency and all its subagencies move together.
4. Click **Save.**

Delete a subagency (level 2 - 9)

Before you delete a subagency, first delete users from the agency. When you delete a subagency, all the agencies below it move up one level.

1. On the Agency page, from the list on the left, click the subagency you want to delete. A list of users appears in the table to the right.
2. Delete the users you want from the subagency by doing these things:
   - Select the subagency.
   - At the bottom of the list of users, click **Edit.**
   - In the **Delete** column for each user, click the X icon, and then click **Save.**
3. Next to the agency, click the Edit icon.
4. In the Edit Subagency window, click **Delete.**

Create a level 1 agency default profile

Your organization administrator can create an agency default profile (ADP) for your organization. The ADP is a predefined agency group that allows agency users limited service when they can't log in to FirstNet. Limited service gives an ADP group's members access to Group PTT calling and group messages with other ADP group members.

An ADP includes 2 types of members:

- **Core members**—Can receive and start PTT calls

- **Agency default members**—Can start PTT calls only

The ADP group prevents other PTT capabilities, including ad hoc group calling, private (1:1) calling, agency default private (1:1) messaging, file sharing, and video streaming.

Each agency user must have a home agency assigned by the organization administrator. The home agency dictates which ADP is applied to the user.

Manage agency users

If you created subagencies, on the Agency page, you need to associate your users with the correct agency. You can also view, add, edit, and delete agency users on the Agency page.

Add 1 or more users to a subagency

You can add the users only from your assigned level 1 agency to its subagencies.

1. On the Agency page, from the list on the left, click the subagency you want to add a user to. A list of users appears in the table to the right.
2. In the bottom right of the user list, click **Edit**.
3. In the agency tree on the right, click the Agency tab and select your entity from the list at the top.

   Note: You can add only the users from the assigned level 1 agency of the selected subagency. Users who are available to add to the agency have an empty checkbox next to their name. The loaned-in mutual control users from another organization are also available. For more information about mutual control, see View and manage mutual aid and mutual control requests.
4. To view a user's profile, click the user's name. In the agency tree, select the users you want to add and click **Add Users**. You can select multiple users.
5. Click **Save**.

View and edit user profiles

1. On the Agency page, from the list on the left, click the agency you want to view. A list of the agency's users appears in the table to the right.
2. In the agency table, select the user you want to view. The **User Profile** window opens.
3. Do any of the following:
   - To lock or unlock the profile, click **Lock User Profile**. If you lock the user profile, some features lock and can't be modified.
   - To view the user's equipment information, click **User Device Information** next to the user's name.
   - To change the user's display name, click **Edit** next to the display name. In the text box, change the display name and click **Save**.

- To view the user history, click **User History** next to the licenses. To edit the home or emergency talkgroup settings, click **Home/Emergency Group**. The **Change Group Setting** window opens. Make your changes and click **Save**.
- To view the full list of talkgroups, click **More Talkgroups**. The **Talkgroup List** window opens.
- To edit the user's ability to do these things, click the **Allowed** or **Disallowed** switch next to each action:
  - Create Ad-hoc Groups
  - First-to-Answer
  - Private Calling & Messaging
  - Ambient Listening
  - Emergency Features
  - User Defined Contact List
  - Be Searched with Contact Search
- To view the contact list, click **Contact List**.
  - To edit the contact list, in the window that appears, click **Edit**. Add or remove the users you want, then click **Save**

4. To close the **User Profile** window, click **List**.

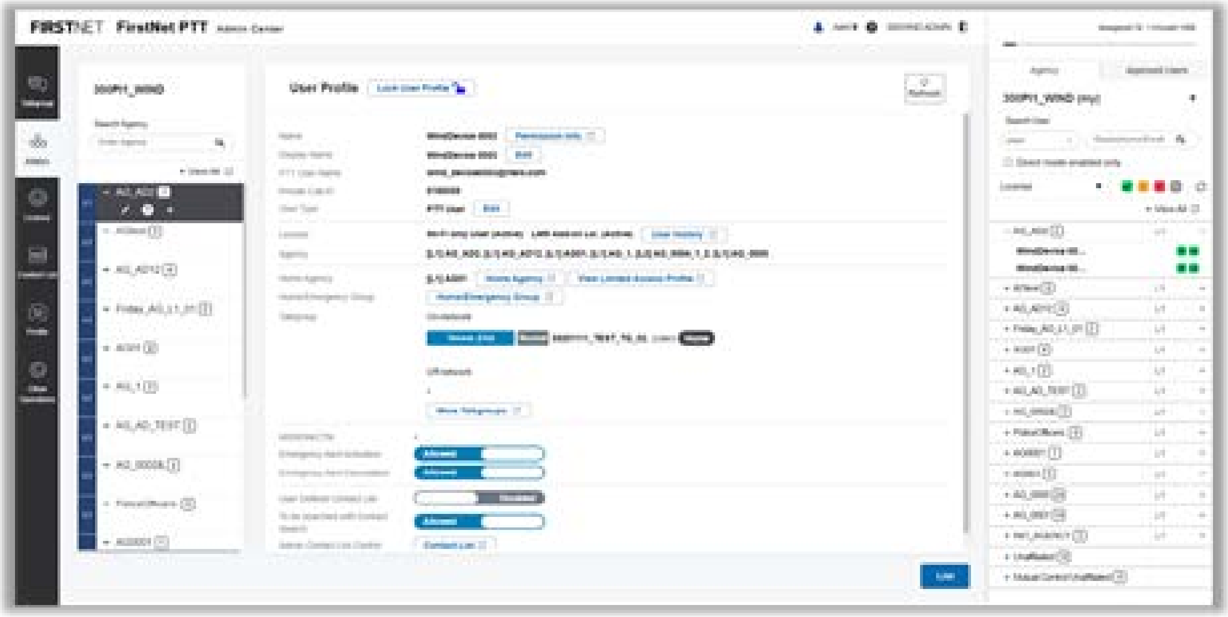


Image 2: User profiles

Remove 1 or more users from an agency

You can delete only the users from the subagencies of your assigned level 1 agency.

1. On the **Agency** page, click the subagency you want to remove the user from, and then click **Edit**.
2. Next to the user or users you want to remove from the agency, click the X icon.
3. Click **Save**.

   Note: The number of users of the parent agency changes when you add or remove users from its subagencies.

Manage push-to-talk licenses

Use the License page to view unused licenses and the status (activated, suspended, canceled, and pending) of assigned licenses. Each user needs a license to use the FirstNet PTT service.

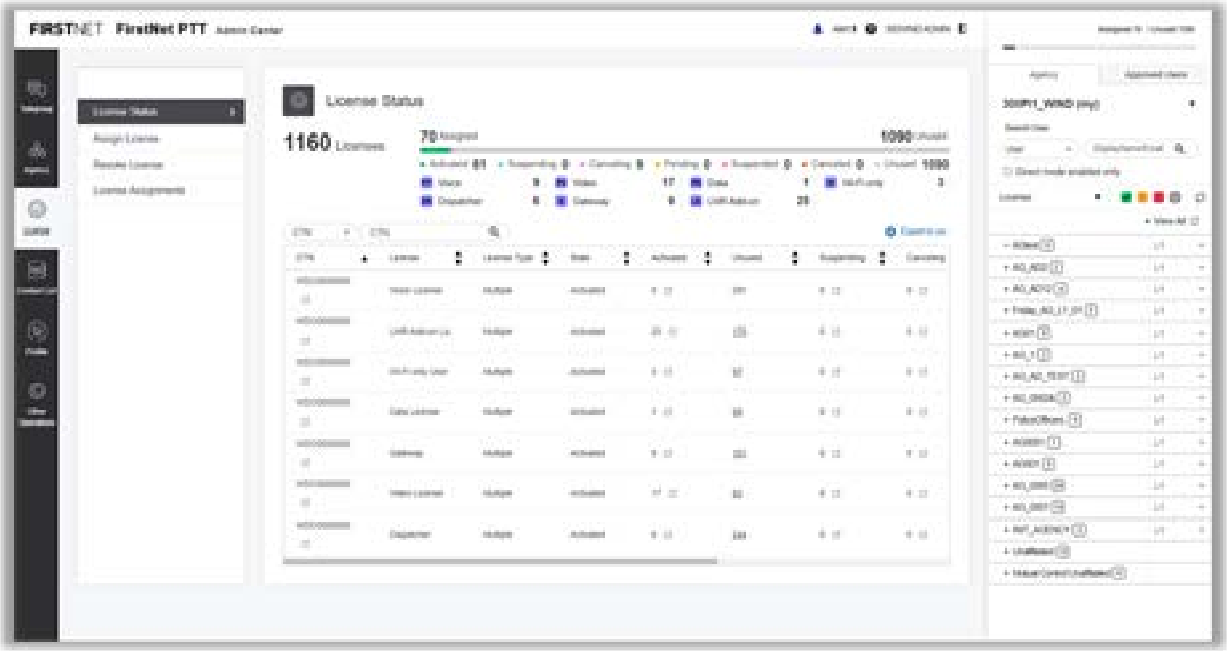


Figure 3: License pages

Understand license types

All FirstNet PTT users (including interoperability profiles) must have a license assigned to them before they can use the PTT service. The following table shows the different license types available in the FirstNet PTT service. Each type enables different functionality.

Note: When licenses are assigned to a user, a tile showing the license type appears next to the user's name in the PTT Admin Tool.

License	Description
FirstNet Push-to-Talk (PTT) subscription (PT)	Provides access to the FirstNet PTT service. This is a paid license.
LMR Interop Add-on (LA)	Allows users to communicate with team members on the LMR network. Users must also have a FirstNet PTT license. This is a paid license.
LMR Push-to-Talk (PTT) Interoperability Profile (G)	Makes an interoperability profile credential operational. Must be assigned a Gateway license. This license is provided free of charge.
Streaming Video (PV)	Allows users to make and receive streaming video calls. Users must also have a FirstNet PTT license. This is a paid license.
Data (PD)	Allows users to send and receive file attachments. This license is included in the FirstNet PTT subscription at no extra charge.

Table 2: FirstNet PTT licenses

View license status

1. From the License page, click **License status.** The license table shows these statistics for each license status:
   - The number of total licenses
   - The number of assigned licenses: Activated, Suspending, Canceling, Pending, Suspended, Canceled
   - The number of unused licenses

     Note: If there aren't any licenses, an error message appears. You'll need to purchase a license.
   - The number of assigned licenses for each license type (shown in license bar above the table)
2. To show or hide the license type in the list, click the License icon.
3. To download the list, click **Export to csv.**
4. To view the status and history of a license, in the table, click the icon next to the wireless

number. The **License status and history** window opens.

Assign a license

You can assign unused licenses to users on the License page by clicking either **Select License** or **Select User.**

When you assign a FirstNet PTT license to a user, we send them a welcome email to let them know their service is set up and to give them their FirstNet PTT administrator's contact information. Make sure to add those users to a talkgroup.

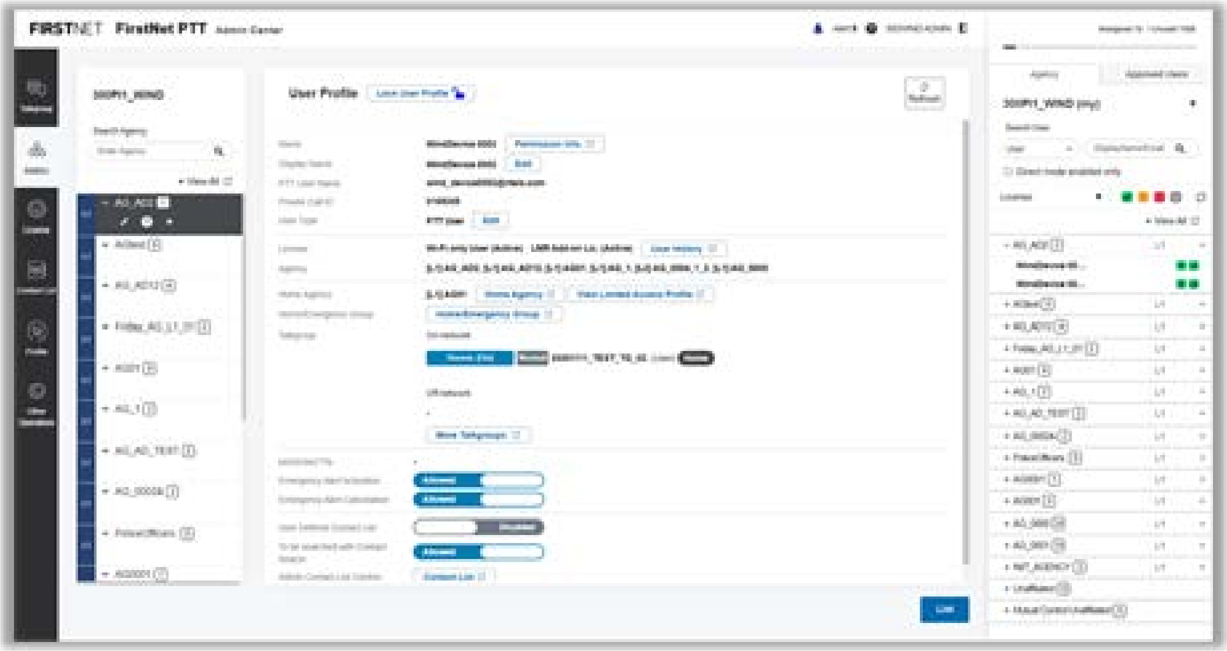


Figure 4: Assign a license

Assign by license type

1. From the License page, click **Assign License.**
2. Click **Select License.**
3. At the top of the **Select License** table, select a license from the list of unused licenses. The list of users you can assign the selected license to appears in the **Select License** table.
4. In the table, select the users and click **Assign.**
5. Click **OK.**

Assign by user

1. From the License page, click **Assign License.**
2. Click **Select User.**
3. Click a user's name in the agency tree area to view the user profile. Click **OK** to close the profile window.
4. Select the user in the agency tree.
5. At the bottom of the agency tree, click **Add User.** The selected user is added in the **Select User** table. The list of licenses that you can assign to the selected user appears in the **Select License** table.
6. To change the selected user, click **Delete** and repeat steps 4 and 5.
7. In the **Select License** table, select the license you want to assign and click **Assign.**
8. Click **OK.**

Revoke a license

If you revoke a license, the license is removed from the user. You can revoke a license by clicking **Select License** or **Select User.**

Revoke by license

1. From the License page, click **Revoke License.**
2. Click **Select License.**
3. In the **Select License** table, select a license from the list of unused licenses. The list of users you can revoke the license from appears in the **Select User table.**
4. In the **Select User** table, select the users you want to revoke the license from and click **Revoke.**
5. In the confirmation window, click **OK.**

Revoke by user

1. From the License page, click **Revoke License.**
2. Click **Select User.**
3. Select the user in the agency tree on the right.

   Note: Users without licenses don't appear in the list.
4. At the bottom of the agency tree area, click **Add Users.** The selected user is added into the **Select User** table. The list of licenses you can revoke from the selected user appears in the **Select License** table.
5. To change the selected user, click **Delete**, and repeat steps 4 and 5.
6. In the **Select License** table, select the license and click **Revoke.**
7. In the confirmation window, click **OK.**

View license assignments

You can search license assignments and view search results based on search criteria, such as date, result, and user.

1. From the License page, click **License assignments.**
2. To set search conditions, click **Search.**
3. To reset search conditions, click **Refresh.**

Search results appear in the **Total list** table. If you need more or fewer licenses, contact your FirstNet representative to adjust your license count accordingly.

Manage talkgroups and talkgroup members

Use talkgroups to define the FirstNet PTT users who your team can communicate with at one time. Create and manage your talkgroups on the Talkgroups page.

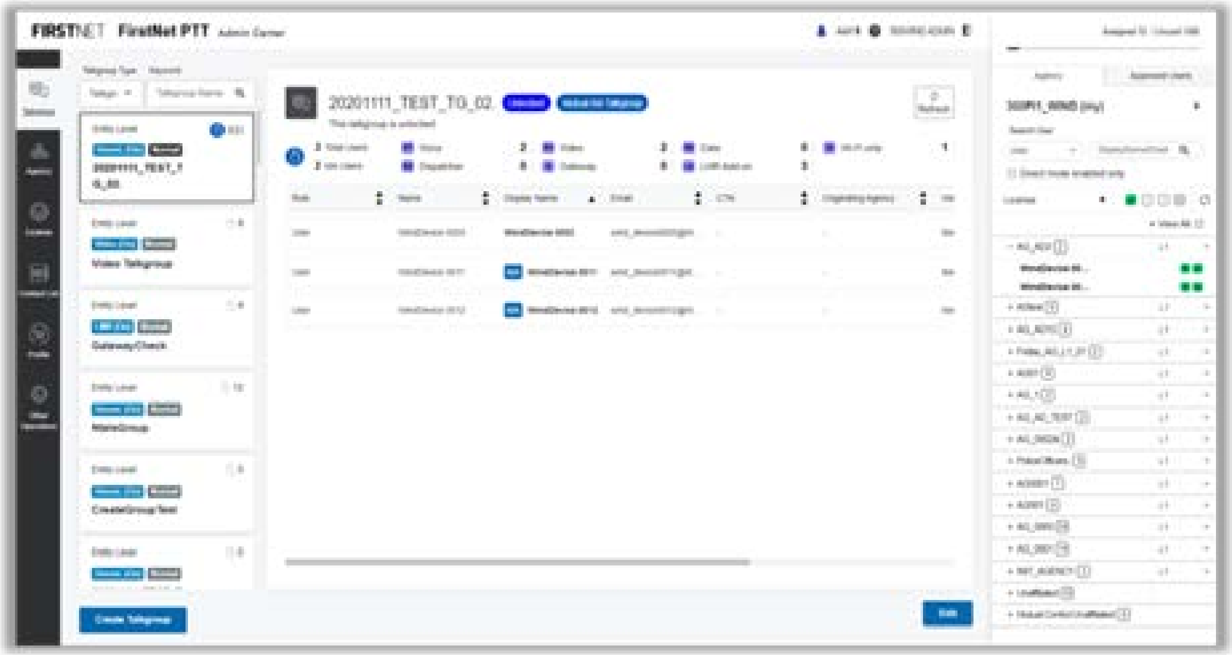


Figure 5: Talkgroup page

About talkgroups

You can create talkgroups in 2 levels: entity level or agency level. You can manage only agency level talkgroups. When you create talkgroups, use a group naming convention that's consistent and meaningful to the users and interagency partners. You can create emergency groups and home groups.

- **Emergency groups**—Used to respond to urgent situations. Includes users who'll respond to the emergency. Don't assign more than 1 emergency group to a single user.
- **Home groups**—Used for typical day-to-day and nonemergency operation for a specific group of users. In most situations, FirstNet PTT defaults to a user's home group.

Manage talkgroups

Talkgroups provide group communications in an organization and are usually defined in the context of agency functions. After you create a group, you can't change its group type.

If you set it as a location-capable talkgroup, member devices report their locations to the system. Only designated users, supervisors, and dispatchers can view location information. Location services allow a supervisor to view others on a map and perform PTT call and messaging functions. Supervisors can also interrupt a call at any time.

To assign supervisors to a location-capable talkgroup, Create a talkgroup or Edit a talkgroup.

Before you create a talkgroup, make sure you've completed these actions:

- Create the agency organizational structure
- Assign users to specific areas in the organization structure
- Assign licenses to the users in the organization

Note: When you assign users to a specific group type, make sure you assign the correct license to use service features. When assigned a license with location services enabled, dispatchers automatically receive location privileges. Removing a dispatcher license removes the dispatcher's location-viewing privileges in all talkgroups.

View a talkgroup

Super administrators can view all talkgroups in their organization. All other administrators can view only the agency-level talkgroups they created.

1. On the **Talkgroup** page, select the talkgroup you want to view.
2. Do any of the following:
   - To show or hide the users assigned to a license type, click the License icon.
   - To refresh the agency user list and the agency tree, click **Refresh.**
   - To display the description of a talkgroup, hover over the talkgroup name and then hover over the Question mark icon that appears.

Create a talkgroup

As a PTT administrator, you can create an agency-level talkgroup.

1. On the Talkgroup page, do 1 of the following:

- If this is your first talkgroup, click **Create**.
- If you already have talkgroups, below the list of talkgroups, click the Plus icon.

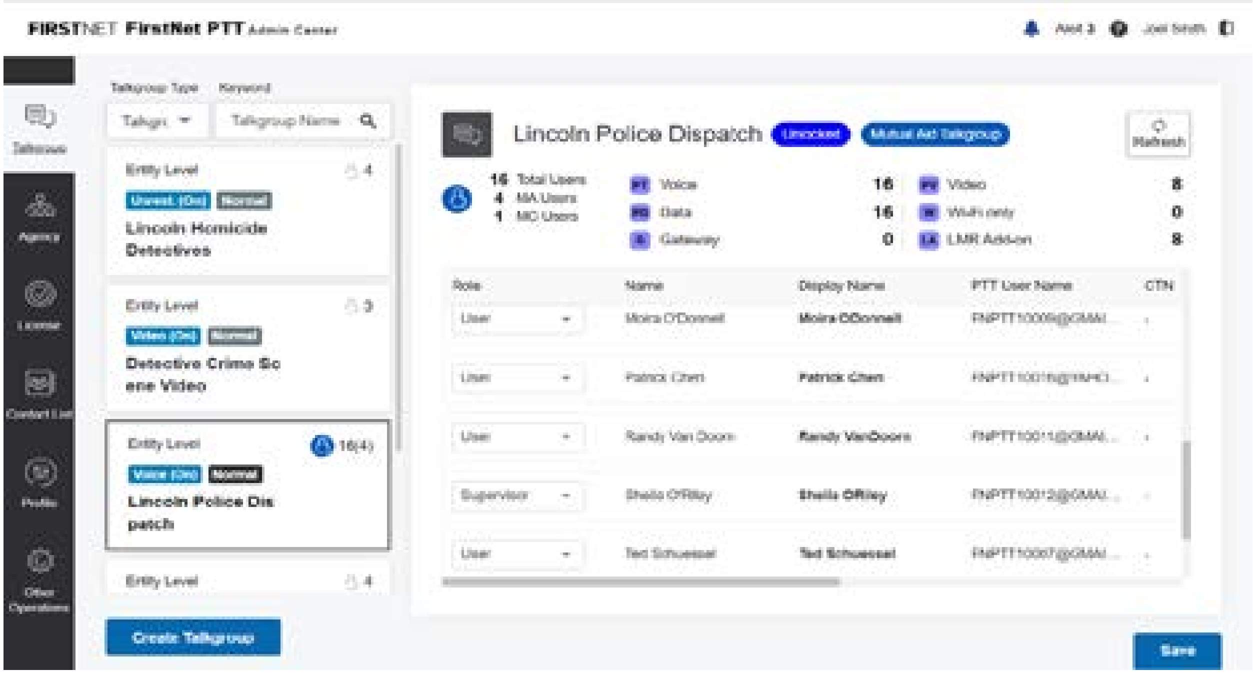
2. Select a talkgroup type:
   - **Unrestricted Group**—Allows PTT voice, texting, file sharing, and video streaming between group members. Doesn't support LMR interoperability. Maximum of 10 video users.
   - **PTT Voice Only Group**—Allows PTT voice and texting between group members. Doesn't support file sharing, video streaming, or LMR interoperability.
   - **PTT Video Only Group**—Allows video streaming between group members. Doesn't support PTT voice, file sharing, or LMR interoperability. Maximum of 10 video users.
   - **LMR Interoperability Group**—Allows PTT voice users to communicate with users on LMR channels. Doesn't support file sharing or video streaming. To create this type of group, you'll need to create an interoperability profile and assign licenses. For more information, see Manage Land Mobile Radio (LMR) and Radio over IP (RoIP) interoperability.

   Note: Users assigned to specific group types still require the correct license to use service features. If you're assigned to a specific group type without a license assignment, it doesn't provide any service functionality.
3. Enter a talkgroup name using these guidelines:
   - Use letters, numbers, and these special characters [+ @ # $ & ( ) , . !]
   - If you use spaces, use only in the middle of the name, not as the first or last character
   - Use a maximum of 80 characters
4. For the nearest server location, enter a 5-digit ZIP Code and click **Search**. If the correct location appears, click **OK.**
5. Select **Normal** or **High priority.** You can't change the priority later.
6. Provide a description up to 200 characters (optional).
7. Click **OK.**

Edit a talkgroup

You can edit agency-level talkgroups you created if you haven't been revoked from the agency.

1. On the **Talkgroup** page, hover over the name of the agency-level talkgroup you want to edit and click the Edit icon. You can search for the talkgroup by type, or enter a keyword in the talkgroup name.
2. Edit the talkgroup name and the server location as necessary.
3. Click **OK.**



Entity Level 4
Unwat. (On) Normal
Lincoln Homicide Detectives

Entity Level 3
Video (On) Normal
Detective Crime Scene Video

Entity Level 16(4)
Voice (On) Normal
Lincoln Police Dispatch

Entity Level 4

Lincoln Police Dispatch Unlocked Mutual Aid Talkgroup

16 Total Users
4 MA Users
1 MC Users

PT Voice	16	PV Video	8
PD Data	16	W WiFi only	0
G Gateway	0	LA LMR Add-on	8

Role	Name	Display Name	PTT User Name	CTN
User	Moira O'Donnell	Moira ODonnell	FNPTT10009@GMAI...	-
User	Patrick Chen	Patrick Chen	FNPTT10016@YAHO...	-
User	Randy Van Doorn	Randy VanDoorn	FNPTT10011@GMAI...	-
Supervisor	Sheila O'Riley	Sheila ORiley	FNPTT10012@GMAI...	-
User	Ted Schuessel	Ted Schuessel	FNPTT10007@GMAI...	-

Figure 6: Select a talkgroup to edit

Delete a talkgroup

You can delete only the agency-level talkgroups you created. Before you delete a talkgroup, you need to remove all the users from the group.

1. On the **Talkgroup** page, click the talkgroup you want to delete. You can search for it by talkgroup type, or enter a keyword in the talkgroup name.
2. To remove all users in the talkgroup, at the bottom right of the user list, click **Edit**, and click the X icon next to each user.
3. Click **Save.**
4. Hover over the name of the talkgroup you want to delete and click the Edit icon.
5. Click **Delete.**

Add a dispatcher profile to talkgroups

Dispatchers need to have their profiles linked with the talkgroups they manage. To connect your talkgroup with the dispatcher console, add a dispatcher profile to your talkgroup.

1. The organization administrator needs to create a dispatcher profile. After the profile is created, it appears in the FirstNet PTT Admin Tool.
2. Add the dispatcher profile to the talkgroups that the dispatcher needs access to. See Edit talkgroup users.

Manage talkgroup members

You can view, add, edit, and delete talkgroup users from the agency-level talkgroups you created.

Add users from your organization to a talkgroup

You can add users to agency-level talkgroups you created.

1. On the **Talkgroup** page, click the talkgroup you want to add a user to. You can search for it by talkgroup type, or enter a keyword in the talkgroup name.
2. In the bottom right of the user list, click **Edit.**
3. Click the **Agency** tab and select your organization from the list at the top. A list of users appears.

   Note: You can add only the users from your assigned level 1 agencies. Users who are available to add to the agency have an empty checkbox next to their name. The loaned-in mutual control users from other entities are also available. For more information about mutual control, see View and manage mutual aid and mutual control requests.
4. To view a user's profile, click their name. In the agency tree, select the users you want to add and at the bottom right,click **Add user** . You can select multiple users.
5. Click **Save.**

Add mutual aid users from another organization to a talkgroup

1. On the **Talkgroup** page, click the talkgroup you want to add a user to. You can search for it by talkgroup type, or enter a keyword in the talkgroup name.
2. In the bottom right of the user list, click **Edit.**
3. In the agency tree on the right, click **Approved users.**
4. Select an organization you requested mutual aid from. A list of approved users appears.
5. To view a user's profile, click the user's name. In the agency tree, select the users you want to add and click **Add user.** You can select multiple users.
6. Click **Save.**

   Note: For more information about mutual aid, see View and manage mutual aid and mutual control requests.

Edit talkgroup users

You can edit the users for the agency-level talkgroups you created. However, you can't edit the users of an agency from which you've been revoked.

1. On the **Talkgroup** page, click the talkgroup you want to edit users in. You can search for it by talkgroup type, or enter a keyword in the talkgroup name.
2. In the bottom right of the user list, click **Edit**.
3. In the user list, you can do any of the following:
   - To change the role, select a role from the list. You can assign supervisors for location-capable talkgroups by changing the role.

     Note: Supervisors can interrupt anyone in the talkgroup, and you can identify them by a blank icon next to the group name.
   - To change the video mode, click **On** or **Off**.
   - To change the voice call permission, select the call permission from the list, if applicable.
   - To change the video call permission, select the call permission from the list, if applicable.

     Note: Video call permissions are unavailable when video mode is turned off.
4. Click **Save**.

Remove 1 or more users from a talkgroup

You can delete users from agency-level talkgroups you created.

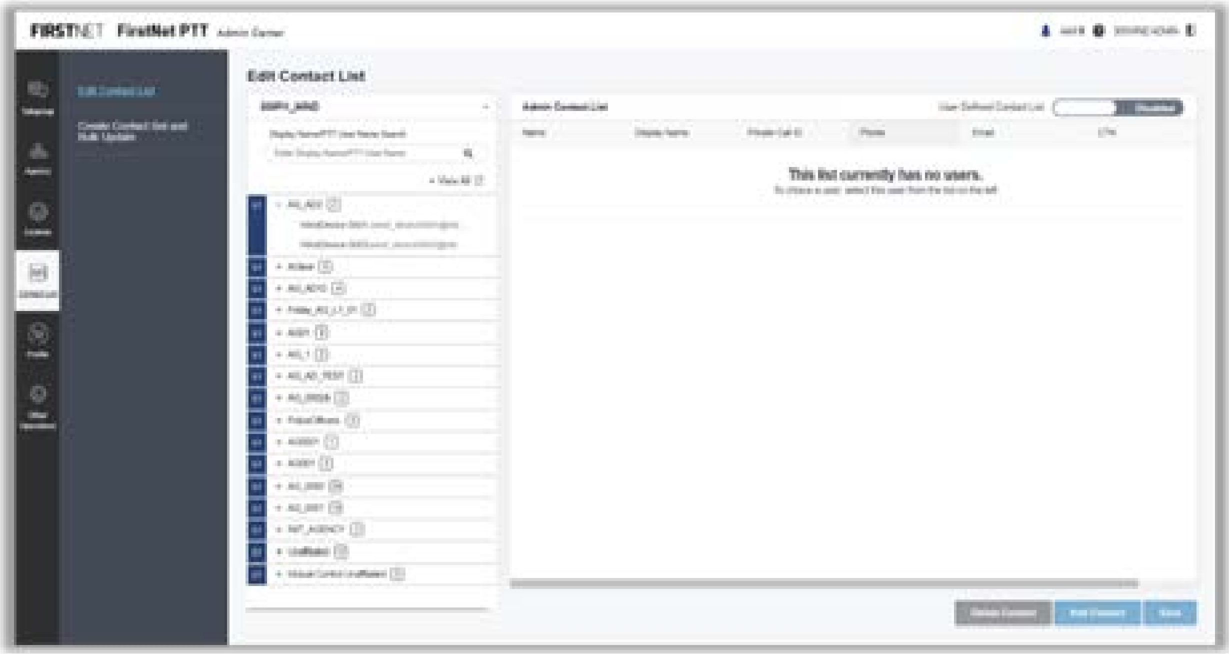
1. On the **Talkgroup** page, click the talkgroup with the user you want to delete. You can search for it by talkgroup type, or enter a keyword in the talkgroup name.
2. At the bottom right of the user list, click **Edit**, and then click the X icon next to the user you want to delete.
3. Click **Save**.

Manage contact lists

You can create, modify, and delete contact lists that are pushed to your FirstNet PTT users' devices.

FirstNet PTT users can make 1:1 calls with contacts on the list. You can specify whether they can also add other contacts to the contacts list on their device.

Manage your Admin contact list
Manage a custom contact set



This list currently has no users.

Figure 7: Contact list pages

Manage your Admin contact list

On the **Contact List** page, you can add, modify, and delete contacts on an Admin contact list. FirstNet PTT users can't edit contacts on their devices.

Add a contact to your Admin contact list

1. From the **Contact List** page, in the list of users, click the user you want to add to your Admin

contacts list.

Note: The list shows only the users of the agencies you're assigned to and their subagencies.

2. Click **Add Contact.**
3. Next to **Display Name**, click **Search.**
4. Search for and select a user, and then click **OK.**
5. In the **Add Contact** window that opens, click **Save.** A list of users appears in the table to the right. The information in this list isn't editable.
6. To change the user defined contact list, click **Disabled** / **Enabled.**
7. Click **Save.**

Delete a contact from your Admin contact list

1. From the **Contact List** page, in the list of users, click the user you want to delete from your Admin contacts list.
2. Check the box next to the contact you want to delete. You can select and delete multiple contacts at one time.
3. Click **Delete Contact.**
4. Click **OK**, and then click **Save.**

Manage a custom contact set

You can create a custom contact set that you can use to bulk update your contact list.

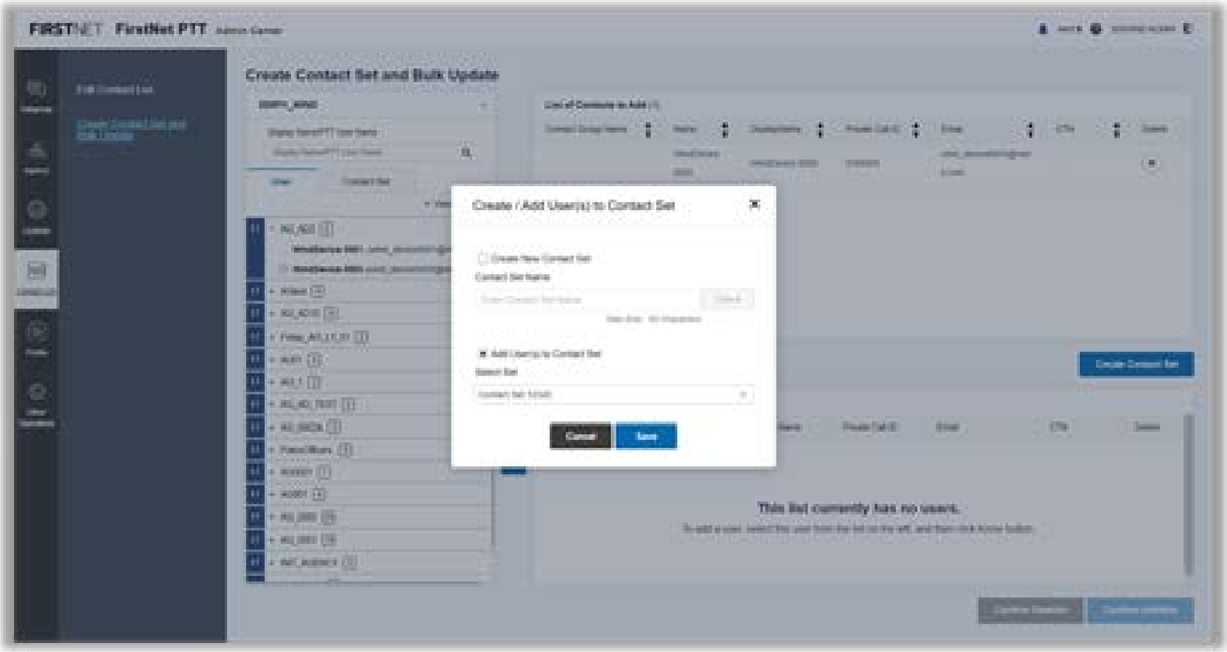

FIRSTNET FirstNet PTT
Create Contact Set and Bulk Update
Create / Add User(s) to Contact Set
Create New Contact Set
Contact Set Name
Add User(s) to Contact Set
Select Set
Cancel
Save
Create Contact Set
This list currently has no users.

Figure 8: **Create / Add User(s) to a Contact Set** window

Create a custom contact

1. From the **Contact List** page, click **Create Contact Set and Bulk Update.**
2. Under the **Display name / email** search field, click the **User** tab.
3. Select the users you want to add to your custom contact list.

   Note: The list shows only the users of the agencies you're assigned and their subagencies.
4. Click **Create Contact Set.**
5. Select **Created New Contact Set.**
6. Enter a contact set name using these guidelines:
   - Use letters, numbers, and these special characters [+ @ # $ & ( ) _ , . !]
   - If you use spaces, use only in the middle of names, not as the first or last character
   - Use a maximum of 80 characters
7. Click **Save.**

Add 1 or more users to a contact list

1. From the **Contact List** page, click **Create Contact Set and Bulk Update.**
2. Under the **Display name / email** search field, click the **User** tab.
3. Select the users you want to add to your custom contact list.
4. Click **Create Contact Set.**
5. Select **Add User(s) to Contact Set.**
6. Select a contact set from the list.
7. Click **Save.**

Edit a contact set name

1. From the **Contact List** page, click **Create Contact Set and Bulk Update.**
2. Under the **Display name / email** search field, click the **Contact Set** tab.
3. Hover over the name of the contact set you want to edit and click the Edit icon.
4. Edit the contact set name.
5. Click **OK.**

Delete 1 or more users from a contact list

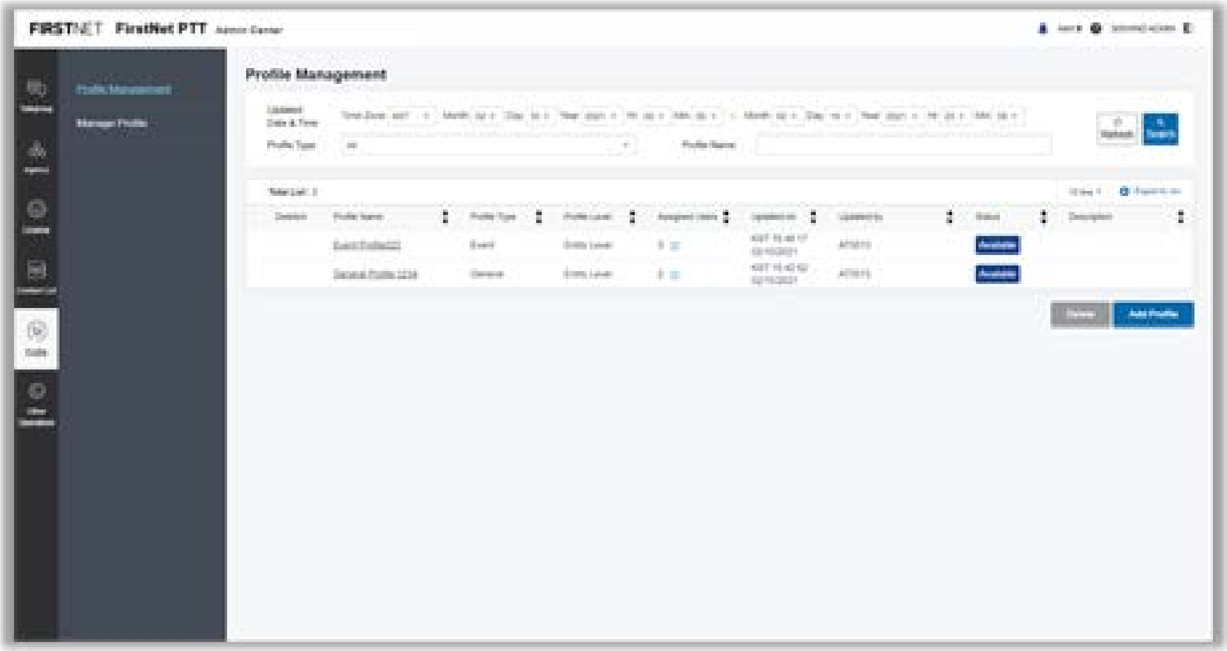
1. From the **Contact List page**, click **Create Contact Set and Bulk Update.**
2. Under the **Display name/email** search field, click the **Contact Set** tab.
3. Select the contact sets or users you want to delete.
4. Click **Delete.**

Manage profiles

On the **Profile Management** page, you can create, modify, and delete general or event profile templates. Use general profile templates to apply a standard set of profile attributes to multiple users at a time. Create event profile templates to use during a specific date and time duration. Event profile templates revert to the original template when the event ends.

Profiles offer flexibility when handling planned changes to standard work arrangements. You can create entity-level or agency-level profile templates. Agency administrators can create and manage only agency-level profile templates. Super administrators can create and manage profile templates at both levels.

Manage profile templates
Manage profile assignments



Deletion	Profile Name	Profile Type	Profile Level	Assigned Users	Updated on	Updated by	Status	Description
	Event Profile222	Event	Entity Level	0	KST 15:40:17 02/10/2021	ATS015	Available	
	General Profile 2224	General	Entity Level	0	KST 15:40:52 02/10/2021	ATS015	Available	

Figure 9: **Profile management** page

Manage profile templates

On the **Profile Management** page, you can create and edit profile templates.

View profile list

You can view only the profile templates you created.

1. From the **Profile** page, enter search terms or keywords for the profile you want to view and click **Search.**
2. Do any of the following:
   - To export the results to a CSV file, click **Export to csv.**
   - To view the list of assigned users of the profile, in the table, click the icon next to the assigned user's number. The **Assigned Users** window opens.
3. To delete profiles, select the profiles you want to delete. Click **Delete** and then click **OK.**

   Note: You can delete only the unavailable profiles.

Create a profile template

1. From the **Profile** page, click **Add Profile.**
2. Enter a profile name using these guidelines:
   - Use letters, numbers, and these special characters: [+ @ # $ & ( ) _ , . !]
   - If you use spaces, use only in the middle of the name, not as the first or last character
   - Use a maximum of 80 characters
3. Select a profile type.
4. To select a target user, click **Select Target User** (optional).
5. Select a user type from the list and click **OK.**
6. If you selected an event profile type in step 4, select a start and end date and time.
7. In the **Feature Settings** section, do any of the following:
   - To add a feature, click the Plus icon.
   - To delete a feature, click the X icon.
   - To add a home or emergency group, select the feature from the list. Click **Select Talkgroup**, select a talkgroup, and click **Save.**
   - To add an emergency alert activation or emergency alert cancellation settings, select the feature from the list, and then click **Allowed** or **Disallowed.**
   - To add a contact list, select the feature from the list, and then click **Search Contacts.** Select a type from the list.
8. If you select **User**, select the users, click **Add Users**, and then click **Save.**
9. If you select **Contact Set**, select the contact sets, click **Add Contact Sets**, and then click **Save.**
10. Provide a description up to 200 characters (optional).

11. Click **Create Profile.**

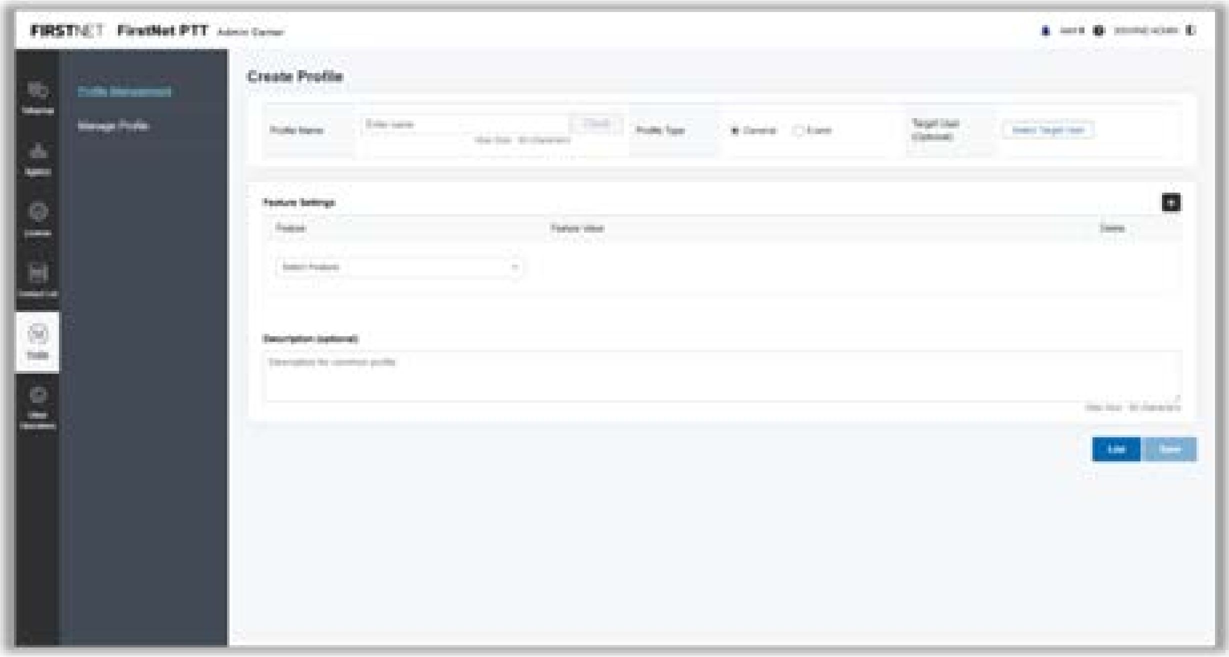


Figure 10: Create a profile

View a profile

You can view and change the status of the profile templates you created. You can also change the activation of the event profile templates. If you were revoked from an agency, you can only disable and deactivate agency-level profile templates you created if they contain users from that agency.

1. From the **Profile** page, click the profile name you want to view.
2. To view the list of assigned users of the profile, in the table, click the icon next to the assigned user's number.
3. To change the status, click **Enabled** or **Disabled**, and then click **OK.**

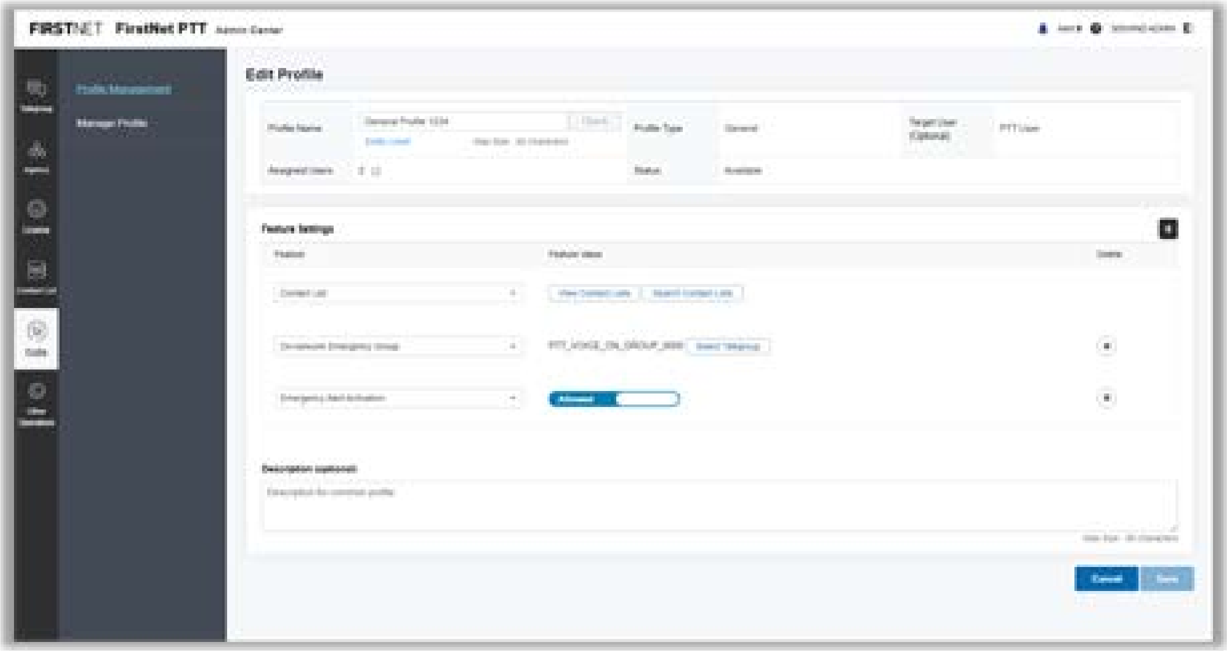
   Note: If you change the status to unavailable, the profile is removed from its assigned users. Unavailable profiles can't be modified or assigned.
4. For the event profile, click **Activated** or **Inactivated.**

   Note: If you change the activation to deactivated, the profile is removed from its assigned users.

Edit a profile

You can edit the agency-level profile templates you created. If you‘ve been revoked from an agency, you can't edit templates assigned to that agency's users.

1. From the **Profile** page, click the profile name you want to view.
2. Click **Edit.**
3. Edit the profile name and the feature settings as necessary.
4. In an event profile, edit the event period.
5. Click **Save.**



Profile Name: General Profile 1234
Profile Type: General
Target User (Optional): PTT User
Status: Available
Contact List
On-network Emergency Group: PTT_VOICE_ON_GROUP_8888
Emergency Alert Activation: Allowed

Figure 11: **Edit Profile** page

Delete a profile

You can delete agency-level profile templates you created. Before you can delete a profile, you need to change the status to unavailable.

1. From the **Profile** page, click the profile name you want to delete.
2. To disable the profile template, click **Enabled**, and then click **OK.**

   Note: If you change the status to unavailable, the profile is removed from its assigned users.
3. Click **Delete.**

Manage profile assignments

On the **Manage Profile** page, you can assign an agency-level profile template you created to users or revoke it from the assigned users.

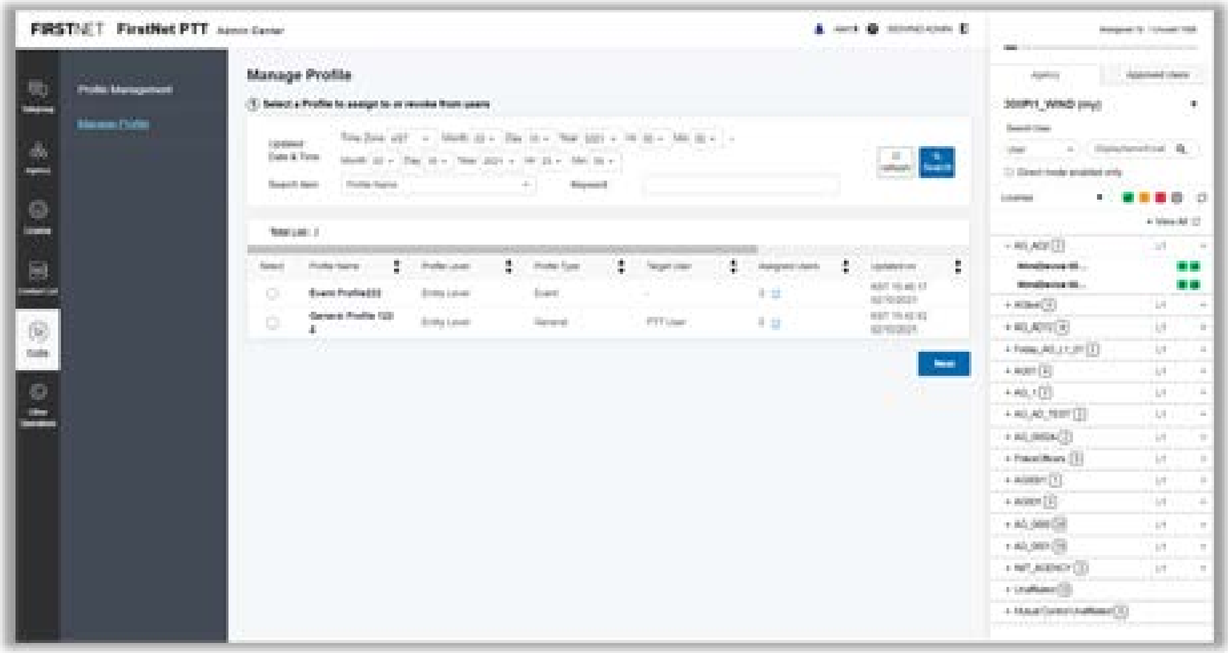


Figure 12: Manage profile assignments

Assign a profile template

1. From the **Profile** page, click **Manage Profile.**
2. Select your search terms or keyword and click Search. Results appear in the table.

   Note: The list shows only the agency-level profile templates you created.
3. To view the list of assigned users of the profile, in the table, click the icon next to the assigned user's number. The **Assigned Users** window opens.
4. Select a profile and click **Next.**
5. In the agency tree on the right, click the **Agency** tab and select your agency from the list at the top. A list of users in that agency appears.

   Note: You can add the users from your assigned level 1 agencies only. Users who are available to add have an empty checkbox next to their name. The loaned-in mutual control users from entities may also be available. For more information about mutual control, see About mutual control in the **Manage mutual aid and mutual control** section.
6. To view a user's profile, click the user's name. The **User Profile** window opens. Click **OK** to

close the window.

7. In the agency tree, select the users you want to add and click **Add Users.** You can select multiple users.
8. Click **Save** to assign the profile. In the confirmation window, click **OK.**

Revoke a profile template

1. From the **Profile** page, click **Manage Profile.**
2. Select your search terms or keyword and click **Search.** Results appear in the table.

   Note: The list shows only the agency-level profile templates you created.
3. To view the list of assigned users of the profile, in the table, click the icon next to the assigned user's number.
4. Select a profile and click **Next.**
5. Click the X icon next to the users you want to delete.
6. Click **Save** to revoke the profile from the deleted users. In the confirmation window, click **OK.**

Use the Other Operations page

Use the **Other Operations** sections to review history of users, licenses, operations, and processing. You can also make mutual aid requests, review the status of requests you've sent, and manage mutual aid requests you've received.

View FirstNet PTT service history
Manage mutual aid and mutual control requests
Manage administrators
Manage permissions
Set up and manage emergency features

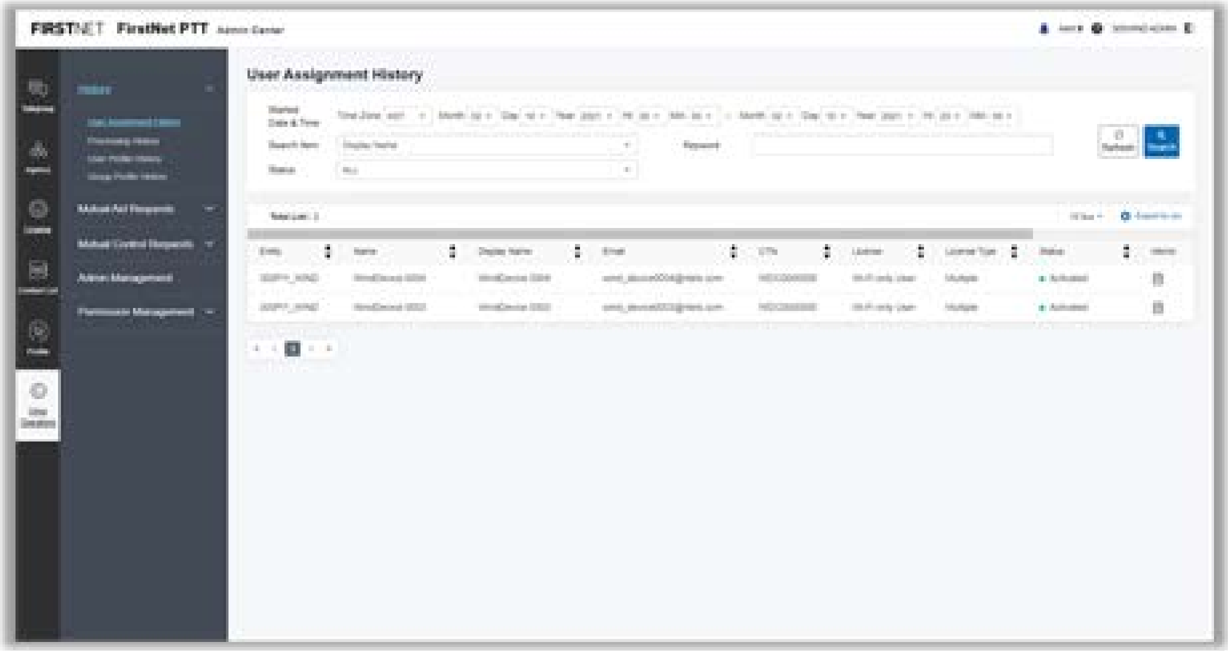


Figure 13: **Other Operations** menu and **User Assignment History** page

View FirstNet PTT service history

The **History** section provides visibility to changes made to the agency's FirstNet PTT service. For example, you can search to see which license types have been applied to or removed from a specific user and when.

View user assignment history

You can view license transactions for your users or agency.

1. From the dashboard, click **Other Operations**, and under **History**, select **User History**.
2. Select your search terms or keyword and click **Search**. Results appear in the table.
3. To export the results to a CSV file, click **Export to csv**.

View processing history

You can run reports using multiple variables to confirm whether specific actions have been processed correctly.

1. From the dashboard, click **Other Operations**, and under **History**, select **Processing History**.
2. Select your search terms or keyword and click **Search**. Results appear in the table.
3. To export the results to a CSV file, click **Export to csv**.

Retry failed process

You can review any transactions that have failed and try to process the transaction again.

1. From the dashboard, click **Other Operations**, and under **History**, select **Processing History**.
2. From the **Result** menu, select **Fail** and click **Search**. A list of failed processes appears in the table.
3. If a transaction result has failed, click **Retry**.
4. If the retry is successful, the **Finished** column shows the date and time when the transaction was completed. The transaction result appears at the top of the list.

Manage mutual aid and mutual control requests

Use the **Mutual Aid Request** or **Mutual Control Request** pages to manage requests you've sent to and received from other agencies.

Existing mutual aid and mutual control partner agencies are listed as favorites. Your favorites list includes agencies with approval pending and agencies with active mutual aid approved users. If your organization opted out of mutual aid or mutual control, you can't make requests, but you can still view request history and incoming mutual aid history.

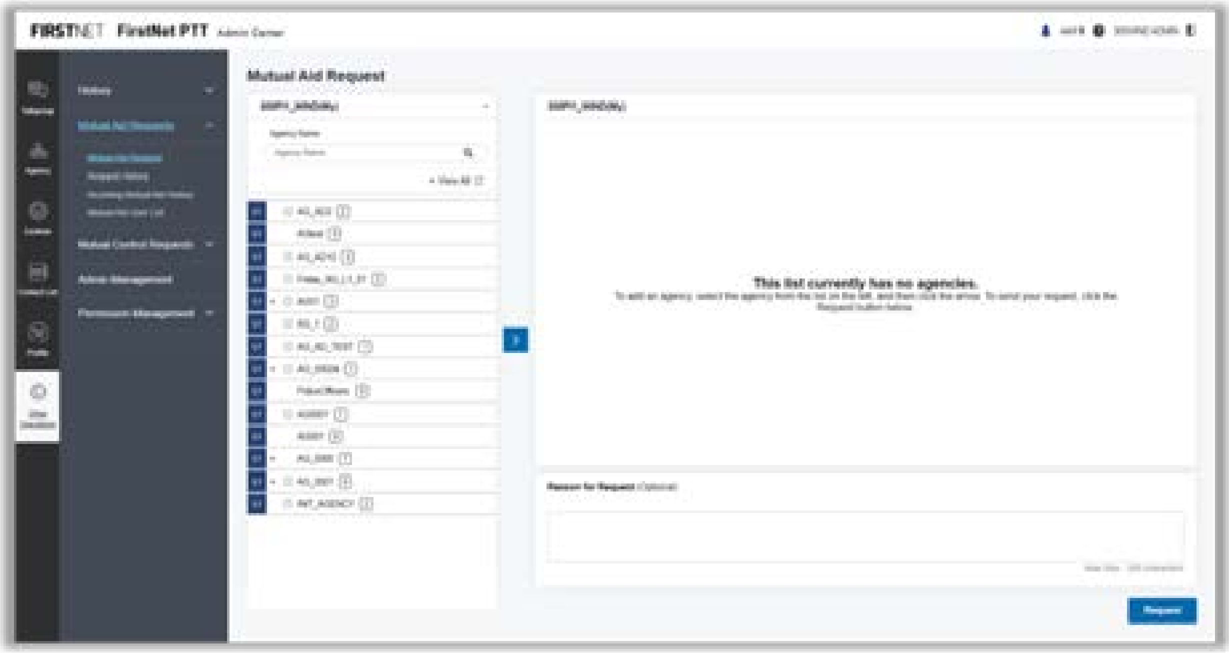


Figure 14: Manage mutual aid requests

About mutual control

Mutual control (MC) allows organizations to delegate user management to administrators in other organizations. For users to be eligible for mutual control, they need to be active and have a valid license. Requesting administrators can manage users, profile group contact lists, mutual aid, and more.

The default super administrator is the only administrator who can do the following:

- Send and receive mutual control requests
- Manage all licenses for services and features

The structure and rules of mutual aid requests apply to mutual control. In addition, the following applies:

- When users are approved for mutual control, they become active in the requesting organization, and the requesting organization has full control of this user.
- When users are released from the requesting organization, they return to their default organization as active users. To manage them further, you need to assign their agency or subagency.
- If a user's license gets revoked after mutual control is approved, they won't be available for mutual control.
- When the users from a different organization are available, the requesting administrator can

manage them like the users in their own organization.

- To assign additional licenses to mutual control users, the requesting administrator needs to contact the users' default organization to assign the appropriate licenses.

Make a mutual aid or mutual control request

1. From the dashboard, click **Other Operations.**
2. Depending on the type of request you want to send, under **Mutual Aid Requests** or **Mutual Control Requests**, select **Mutual Aid Request** or **Mutual Control Request.**
3. Select the organization you want to make the request to.

   Note: If there aren't any approved users of mutual aid, an error message appears.
4. Select the agency.

   Note: Agencies without users and agencies that opted out can't be selected. The users without licenses or the loaned-out mutual control users also won't be included in the request.
5. Click the arrow in the center of the page to move the selected agency to the right area.
6. To delete the selected users, click **Delete.**
7. Enter the reason for request and click **Request** in the bottom right.
8. In the window that appears, view the administrator list and click **OK** to submit the request.

The request is routed to the FirstNet PTT administrators of the other organization and appears on their FirstNet PTT Admin Tool dashboard. We send an email notification to let them know a request is waiting.

View request history

You can view your mutual aid and mutual control request history to see whether your requests have been accepted, rejected, or if no action has been taken by the target entity. If accepted by the other organization, the FirstNet PTT users they make available appear on the **Approved Users** tab of the **Talkgroup** page. You can include these users in your talkgroups.

1. From the dashboard, click **Other Operations.**
2. Under **Mutual Aid Requests**, select **Requesting History**, or under **Mutual Control Requests**, select **Request History.**
3. Set search conditions and click **Search.**
4. In the **Status** column, next to the agency you want to view, click the Window icon for a request that hasn't been acted on yet.
5. In the window that opens, view the request status and click **OK.**
6. To cancel a request that hasn't been acted on yet, click **Cancel.**
7. To cancel your access to another agency's FirstNet PTT users, click **Return Users.** Select the users and click **OK** to finish the mutual aid to release them.

   Note: If approved FirstNet PTT users are revoked by the lending agency, they're automatically removed from your talkgroups.

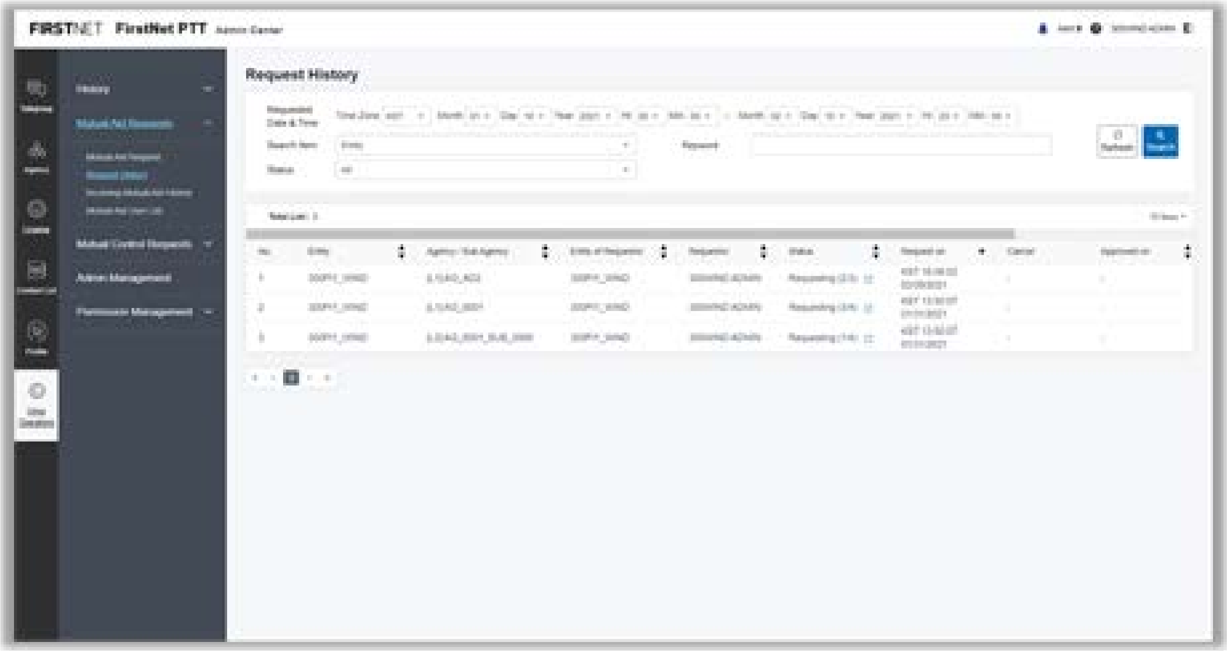


Figure 15: **Request History** page

View the history of incoming requests

1. On the dashboard, click **Other Operations.**
2. Under **Mutual Aid Requests**, select **Incoming History**, or under **Mutual Control Requests**, select Incoming **Mutual Control History.**
3. Set search conditions and click **Search.**
4. Do 1 of these things:
   - To approve the request, in the **Approve** column, click **Approve**, select the users you want and then click **OK.**

     Note: You can approve all or some of the requested users. If the request is partially approved, the other administrators can approve or reject the remaining users. You can approve or reject only users only one time, but you can revoke the approved users by yourself or other administrators at any time.
   - To reject the request, in the **Reject** column, click **Reject.**
   - To finish the mutual aid or mutual control, in the **Revoke** column, click **Revoke**, then select the users you want and click **OK** to remove them from the other agency's talkgroups.

     Note: A request that's been approved stays in place until either the requesting or approving FirstNet PTT administrator revokes the request.

Manage administrators

On the **Admin Management** page, you can assign or revoke super or agency administrators.

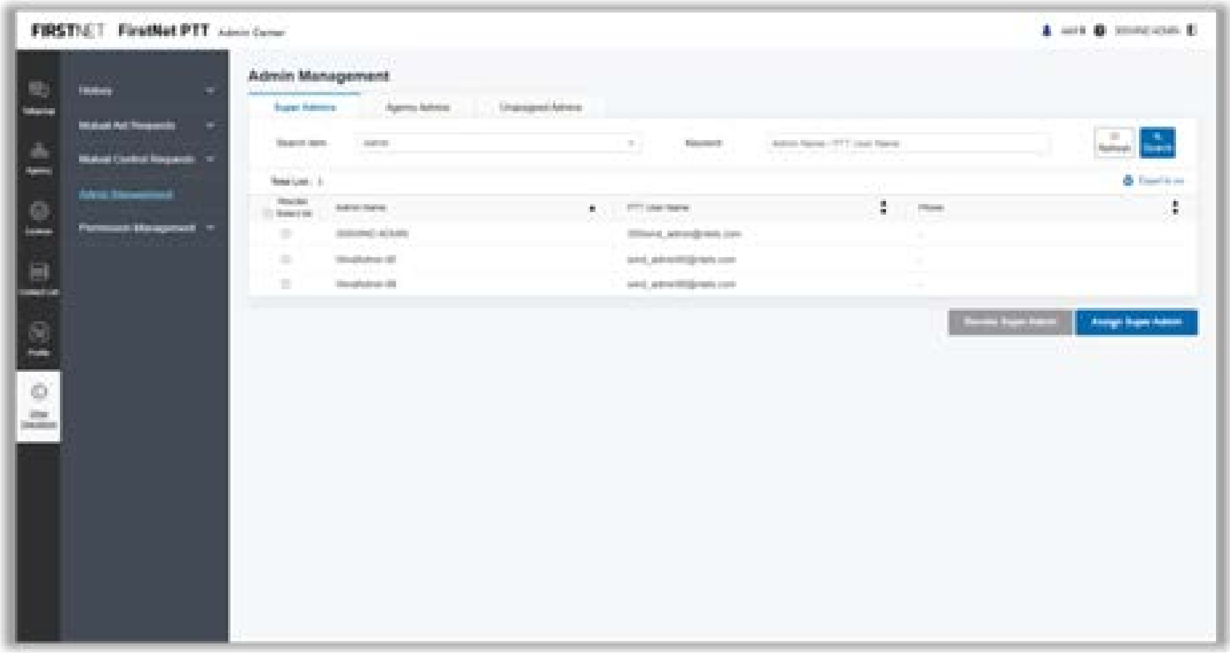


Figure 16: **Admin Management** page

Assign super administrators

If you're the first unassigned administrator to log in to an organization that has no super administrators, you can assign yourself and other users to the super administrator role. If another unassigned administrator logs in and assigns super administrator roles before you do, you won't be able to assign yourself or other users to that role.

Note: If you assign agency administrators to the super administrator role, they'll be removed from all assigned agencies and lose the agency administrator privileges.

1. From the dashboard, click **Other Operations.**
2. Click **Admin Management.**
3. On the **Super Admin** tab, click **Assign Super Admin.** Or, to see all unassigned administrators, on the **Unassigned Admin** tab, click **Assign Super Admin.**
4. Select the administrators you want to assign and click **Assign.**

   Note: You can assign up to 100 super administrators.
5. In the confirmation window, click **OK.** The super administrators you assigned appear in the

administrator list on the **Super Admin** page.

Revoke super administrators

Note that if you revoke yourself, you'll lose your permissions and be redirected to the dashboard.

1. From the dashboard, click **Other Operations.**
2. Click **Admin Management.**
3. On the **Super Admin** tab, select the administrators you want to revoke and click **Revoke Super Admin.**

Assign agency administrators

1. On the dashboard, click **Other Operations.**
2. Click **Admin Management.**
3. On the **Agency Admin** tab, click **Assign Agency Admin.**
4. Select the administrators you want to assign, select the agencies you want to assign them to, and then click **Assign.**

Assign or unassign agency administrators

1. On the dashboard, click **Other Operations.**
2. Click **Admin Management.**
3. On the **Agency Admin** tab, and in the table, click the icon next to the administrator's name. The **Edit Assigned Agencies** window opens.
4. Do any of the following and then click **Save**:
   - Select the agencies you want to assign the administrator to.
   - Deselect the agencies you want to remove the administrator from.

Revoke agency administrators

Note that if you revoke yourself, you'll lose your privileges and be redirected to the dashboard.

1. From the dashboard, click **Other Operations.**
2. Click **Admin Management.**
3. On the **Agency Admin** tab, select the administrators you want to revoke and click **Revoke Agency Admin.**

Manage permissions

On the **Permission Management** page, you can manage permissions of user profile features, group profile features, and email notifications.

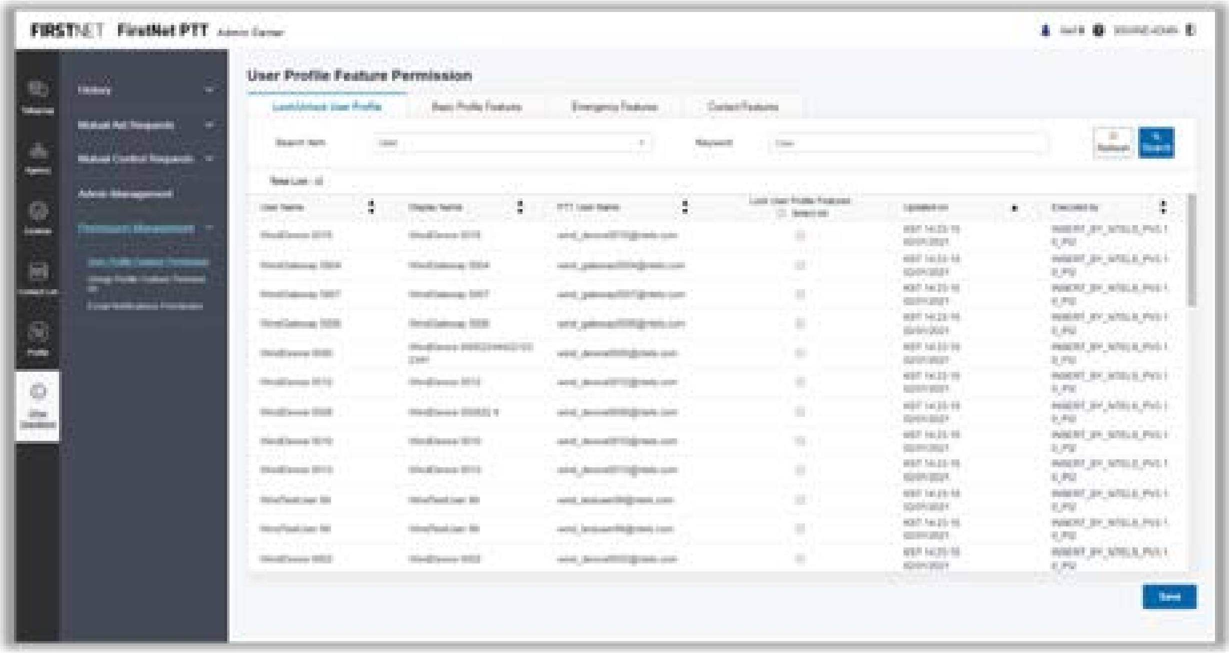


Figure 17: **Lock/Unlock User Profile** tab of the **User Profile Feature Permission** page

Lock or unlock user profile feature permissions

1. From the dashboard, click **Other Operations.**
2. Under **Permission Management**, click **Lock/Unlock User Profile.**
3. Set search conditions and click **Search.**
4. Select the user whose profile you want to lock. To unlock a user's profile, deselect the user.

   Note: To select or deselect all, check or uncheck the **Select All** box.
5. Click **Save.** In the confirmation window, click **OK.**

Manage basic user profile feature permissions

1. From the dashboard, click **Other Operations.**
2. Under **Permission Management**, click **Basic Profile Features.**
3. Set search conditions and click **Search.**
4. To enable a basic profile feature, select the users for the feature. To disable the feature, deselect the users.

   Note: To select or deselect all, check or uncheck the **Select All** box.
5. Click **Save.** In the confirmation window, click **OK.**

Manage emergency user profile feature permissions

1. From the dashboard, click **Other Operations.**
2. Under **Permission Management**, click **Emergency Profile Features.**
3. Set search conditions and click **Search.**
4. To allow an emergency profile feature, select the users for the feature. To disallow the feature, deselect the users.

   Note: To select or deselect all, check or uncheck the **Select All** box.
5. Click **Save.** In the confirmation window, click **OK.**

For more information about emergency features for your organization and agencies, go to the Set up and manage emergency features section.

Manage contact user profile feature permissions

1. From the dashboard, click **Other Operations.**
2. Under **Permission Management**, click **Contact Profile Features.**
3. Set search conditions and click **Search.**
4. To enable or allow a contact profile feature, select the users for the feature. To disable or disallow the feature, deselect the users.

   Note: To select or deselect all, check or uncheck the **Select All** box.
5. Click **Save.** In the confirmation window, click **OK.**

Manage email notifications permissions for administrators

1. From the dashboard, click **Other Operations.**
2. Under click **Permission Management**, click Email Notifications Permissions.
3. Click **Admin.**
4. To turn on an email notification, check the box. To turn off the notification, uncheck the box.
5. Click **Save.** In the confirmation window, click **OK.**

Manage email notifications permissions for users

Mutual aid and mutual control notifications permissions can’t be changed.

1. From the dashboard, click **Other Operations.**
2. Under **Permission Management**,click **Email Notifications Permissions.**
3. Click **User.**
4. Set search conditions and click **Search.**
5. To turn on an email notification, select the users for the notification. To turn off the notification, deselect the users.

Note: To select or deselect all, check or uncheck the **Select All** box.

6. Click **Save.** In the confirmation window, click **OK.**

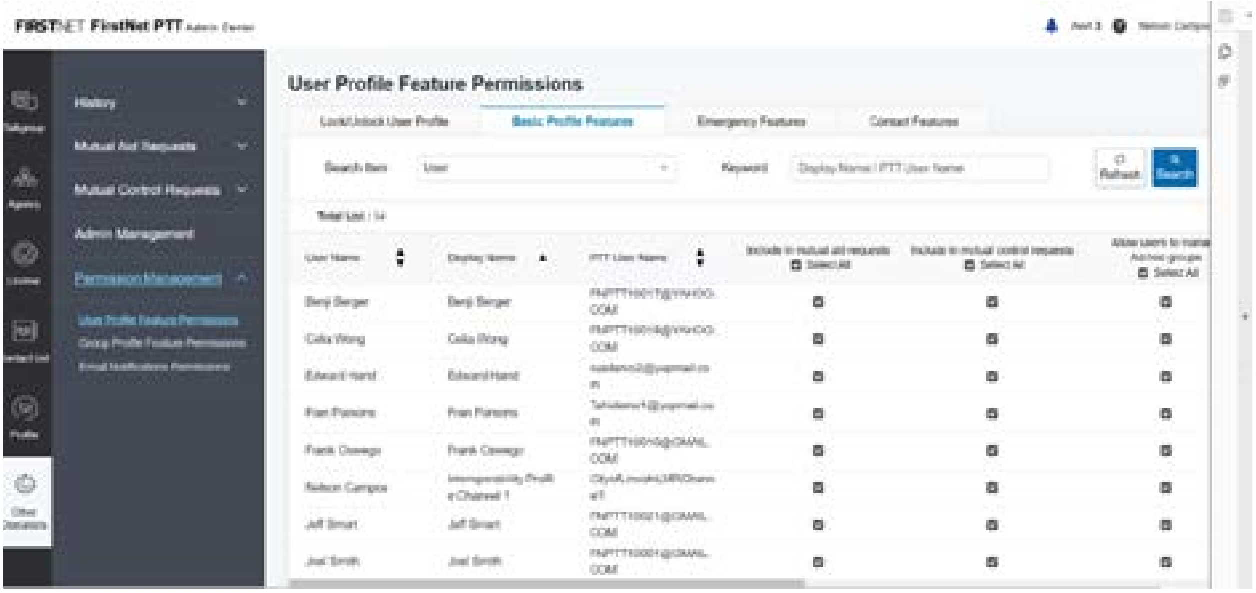
Manage mutual aid and mutual control permissions for users

To allow or restrict specific users from mutual aid and mutual control requests:

1. From the dashboard, click **Other Operations.**
2. Under **Permission Management**, click **User Profile Feature Permissions.**
3. From the **Basic Profile Features** tab, select or deselect the boxes under Include in mutual aid requests and Include in mutual control requests.

   Note: You can only edit users in your span of control.

When users are opted-in to mutual aid or mutual control, you can view them in the **Mutual Aid/ Mutual** control requested list.



User Profile Feature Permissions

Search Item: User

Keyword: Display Name / PTT User Name

Total List : 14

User Name	Display Name	PTT User Name	Include in mutual aid requests ☑ Select All	Include in mutual control requests ☑ Select All	Allow users to mana Ad-hoc groups ☑ Select All
Benj Berger	Benj Berger	FNPTT10017@YAHOO.COM	☑	☑	☑
Celia Wong	Celia Wong	FNPTT10018@YAHOO.COM	☑	☑	☑
Edward Hand	Edward Hand	[illegible]@yopmail.com	☑	☑	☑
Fran Parsons	Fran Parsons	[illegible]@yopmail.com	☑	☑	☑
Frank Oswego	Frank Oswego	FNPTT10010@GMAIL.COM	☑	☑	☑
Nelson Campos	Interoperability Profile Channel 1	[illegible]	☑	☑	☑
Jeff Smart	Jeff Smart	FNPTT10021@GMAIL.COM	☑	☑	☑
Joel Smith	Joel Smith	FNPTT10001@GMAIL.COM	☑	☑	☑

Figure 18: User Profile Feature Permissions page

When the organization level setting is set to opt-out, the opt-in and out setting doesn't display in user profile. However, if an agency opted out, the user setting won't change because the user can be included in multiple agencies.

To view the update history for mutual aid or mutual control participation:

1. From the dashboard, click **Other Operations.**

2. Under **History**, click **User Profile History.** The update history appears in the user list on the **Basic Profile Features** tab.
3. To opt out individual users, edit their profile.

Set up and manage emergency features

The FirstNet PTT Admin tool includes a variety of emergency features that your users and dispatchers can access. The default setting for all emergency features is On.

User emergency features:

- Start emergency calls
- Activate emergency alert
- Cancel emergency alerts
- Cancel emergency alerts for other users (Supervisor only)

Dispatcher emergency features:

- Start emergency calls
- Cancel emergency alerts for other users
- Ambient listening

Customize emergency features

You can set user and dispatcher emergency features on FirstNet PTT to be consistent with your LMR system, so responder training is the same across systems.

You can edit individual user settings on each user’s profile page, or you can edit all users’ settings at once.

Note the following:

- If you turn off your organization’s emergency services, all emergency features for users and dispatchers are turned off and can’t be changed individually.
- When a user’s Emergency alert activation and Cancel emergency alert features are turned off, that user can’t start emergency calls but can still belong to emergency groups and receive calls and messages.
- Dispatchers and supervisors with Emergency alert cancellation permissions can cancel alerts they initiate and alerts initiated by others. You can’t turn off their ability to cancel alerts initiated by others.
- When mobile users have Emergency alert cancellation permissions, they can cancel only the emergency alerts they initiate.

Enable hot mic for emergency calls

You can set the Emergency call feature to allow a hot mic. You can use different settings across agencies and subagencies in your organization. The default setting doesn't allow hot mic.

- **Hot mic**—Call opens the mic for an adjustable number of seconds
- **Default**—Call starts as a standard group call

Specify initial floor control for emergency calls

The emergency call feature lets you specify how calls are started and how the floor is granted to the user declaring an emergency. You can set up this feature on an organization level or a group level. If you set it up at an organization level, you can customize the settings for a group.

You can choose between these 2 emergency call start options:

- **Implicit**—The floor is taken by the call originator at the start of the call. When the originator presses the emergency key, a hot mic is opened for a set amount of time. You can customize this duration for 10, 15, 20, 30, or 60 seconds.
- **Explicit**—Users must take an action to hold the floor. They can either push and hold the PTT side key or tap the PTT key on a touchscreen. This is the default setting when an organization is created. When explicit is selected, the menu for implicit is disabled.

Edit emergency call permissions for multiple users at 1 time

1. From the dashboard, click **Other Operations.**
2. Under **Permission Management**, select **User Profile Feature Permissions.**
3. Click the **Emergency Features** tab.
4. Check or uncheck the boxes under the emergency features you want to enable or disable.

Edit organization-level emergency call settings

If you're a super administrator, you can change the emergency feature settings at an organization level on the agency page.

1. On the agency page, next to your organization's name at the top left, click the Edit icon.
2. On the **Edit Entity Settings** window, change emergency call options.
3. Click **Save.**

To view a user's emergency features update history:

1. From the dashboard, click **Other Operations.**
2. Under **History**, select **User Profile History**.
3. On the user profile history page, click the **Emergency Features** tab.

Manage Land Mobile Radio (LMR) and Radio over IP (RoIP) interoperability

FirstNet PTT interoperates with two-way LMR systems to allow group communications between the LMR system and LTE FirstNet PTT devices.

LMR Interop overview

LMR Interop allows FirstNet PTT users to talk with LMR users. Connectivity is established through an RoIP gateway on the customer's premises. The RoIP gateway converts two-way LMR calling to FirstNet PTT calling and vice versa.

The setup for LMR Interop requires steps action on FirstNet Central and at the customer premises.

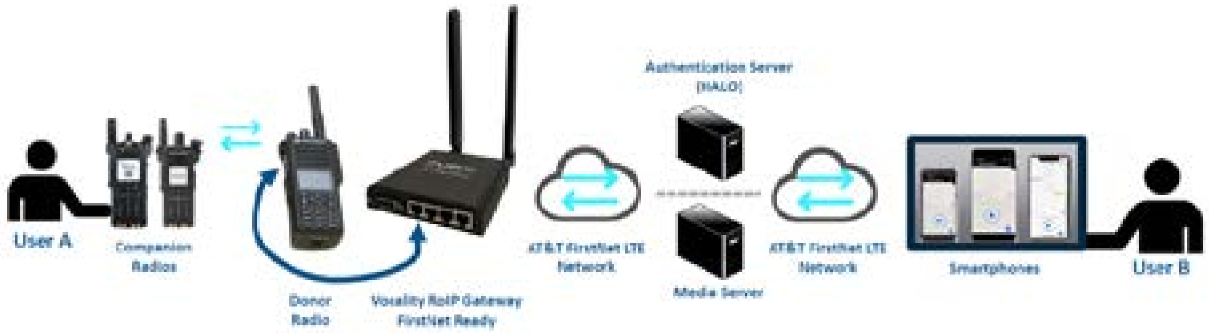


Figure 19: LMR Interop overview

To set up the RoIP gateway for LMR to LTE Interop access:

On FirstNet Central

Create an interoperability profile. This credential is an identifier used to associate an RoIP gateway port/LMR channel to a FirstNet PTT LMR talkgroup.

1. After it's created, the interoperability profile appears in the FirstNet PTT Admin Tool.
2. Make sure a gateway license (LMR Interop Port License) is assigned to the interoperability

profile.

3. Create a FirstNet PTT LMR talkgroup that corresponds to your LMR channel.
4. Add the interoperability profile to the talkgroup.
5. Add FirstNet PTT users to the LMR Interop talkgroup. Each FirstNet PTT user must have an LMR Interop Add-on license.

   Note: Creating an LMR Interop talkgroup that consists only of FirstNet interoperability profiles isn't recommended.

At the customer's premises

1. The interop installer or gateway sponsor installs the RoIP gateway, donor radios, and cabling.
2. The donor radio is tuned to the appropriate LMR channel and connected by a cable to a specific port on the RoIP gateway.
3. The interop installer or gateway sponsor connects the laptop to the gateway and enters the interoperability profile and password to activate that port.

After the hardware is set up, and the same interoperability profile is associated to the port and to the LMR Interop talkgroup, FirstNet PTT users and LMR users can talk with each other.

Set up LMR Interop equipment

Most often, an internal IT or LMR support resource is required on site to perform or help with LMR Interop installation. FirstNet PTT administrators are responsible for setting up LMR Interop in the FirstNet PTT Admin Tool. We recommend that you choose from the following installation services:

- Remote installation
- LMR dealer
- Your own LMR or IT support resource

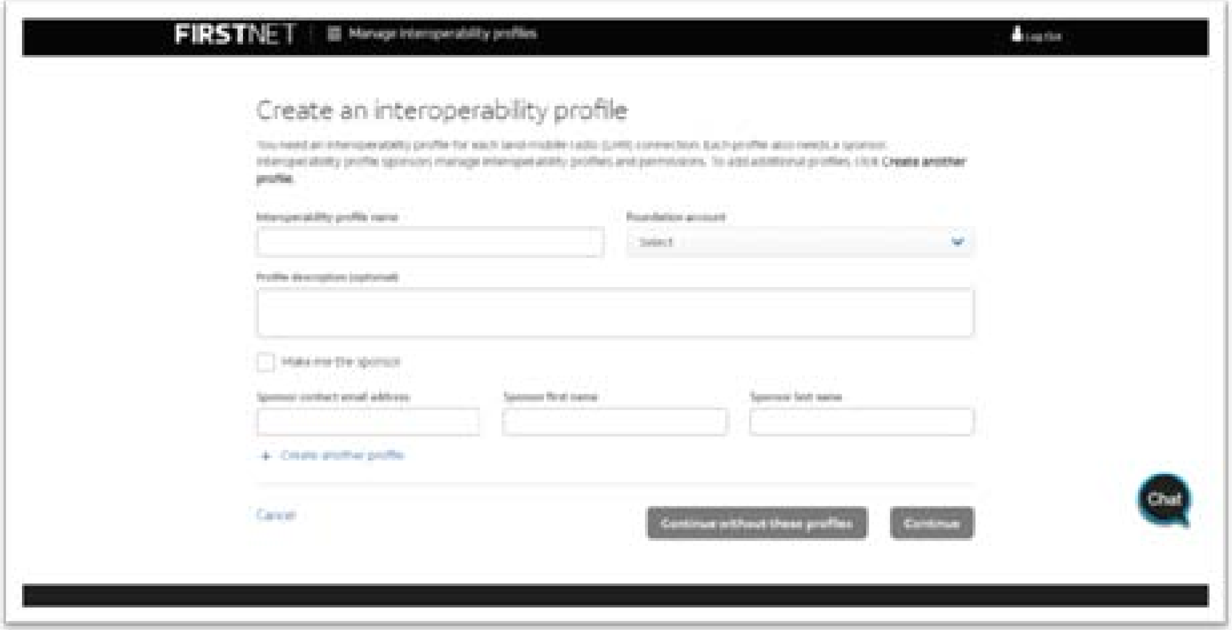
Overview of LMR Interop equipment setup

These steps provide a basic outline for setting up LMR Interop equipment.

1. Connect your RoIP gateway to your PC with an Ethernet cable.
2. Using a web browser on your PC, connect to the RoIP address.
3. Log in using the RoIP gateway administrator credentials.

FirstNet PTT interoperability profiles

A FirstNet interoperability profile is an identifier used to associate a specific port on the RoIP gateway with a specific talkgroup in the FirstNet PTT service.



Create an interoperability profile

You need an interoperability profile for each land mobile radio (LMR) connection. Each profile also needs a sponsor. Interoperability profile sponsors manage interoperability profiles and permissions. To add additional profiles, click **Create another profile**.

FIRSTNET
Manage interoperability profiles
Log Out
Interoperability profile name
Foundation account
Select
Profile description (optional)
□ Make me the sponsor
Sponsor contact email address
Sponsor first name
Sponsor last name
+ Create another profile
Cancel
Continue without these profiles
Continue
Chat

Figure 20: **Create an interoperability profile** page

To associate LMR users with FirstNet PTT users, you need the following:

- A FirstNet interoperability profile
- 1 RoIP gateway port for each LMR channel
- A corresponding LMR Interop talkgroup

Associate LMR users with FirstNet PTT users

To associate LMR users with FirstNet PTT users:

1. Create the interoperability profile in FirstNet Central.
2. Configure a port on the RoIP gateway with the interoperability profile.
3. Add the interoperability profile to the LMR Interop talkgroup.

Manage your FirstNet interoperability profile

Organization administrators can manage interoperability profiles.

1. From FirstNet Central, click **Manage Users**.
2. At the top of the page, click **User Management**, select **Manage Interoperability Profiles**, and then select **View Profiles**.
3. On the **Manage Interoperability Profiles** page, do any of the following:

- Search for and view profiles
- View sponsor email addresses
- View profile status

4. To see full details about a profile, click its name.
5. To create a profile from this page, click **Add Interoperability Profile**, and then follow steps 4 - 6 in the next procedure.

Create a FirstNet interoperability profile

1. From FirstNet Central, click **Manage Users.**
2. At the top of the page, click **User Management**, select **Manage Interoperability Profile**, and then select **Add Profiles.**
3. Enter a name for your interoperability profile and select the foundation account it belongs to.
4. Enter a description (optional).
5. Check the **Use me as the sponsor** box or enter the sponsor's email address and name.
6. Click **Continue.** A success message appears, and an activation email is sent to the sponsor.

After the sponsor clicks the link in the email and completes the process, the profile status shows as **Active.**

Assign a Gateway license (LMR Interop Port license)

Each FirstNet interoperability profile must have a Gateway license assigned to it. You assign licenses in the FirstNet PTT Admin Tool. You can order a Gateway license from your FirstNet representative.

Assign by license

1. From the dashboard, click **License.**
2. Click **Assign License.**
3. At the top of the **Select License** table, select a gateway license from the list of unused licenses. The list of users you can assign the selected license to appears at the bottom of the table.
4. In the table, select 1 or more users you want to assign the license to and click **Assign.**
5. In the confirmation window, click **OK.**

Assign by user

1. From the dashboard, click **License.**
2. Click **Assign License.**
3. Click **Select User.**
4. In the agency tree area to the right, select a user whose user type is LMR Interface User (LMR gateway).

Note: To see a user's type, click the user's name to view the user's profile. When you're done, click OK to close the profile window.

5. At the bottom of the agency tree, click **Add user**. The selected user is inserted in the **Select User** table. The list of licenses that you can assign to the selected user appears in the **Select License** table.
6. You can do either of the following, if necessary:
   - To change the selected user, click Delete.
   - To add more users, repeat steps 4 - 6.
7. In the **Select license** table, select **Gateway license** from the list and click **Assign.**
8. In the confirmation window, click **OK.**

Manage an LMR Interop talkgroup in FirstNet PTT

An LMR Interop talkgroup is a group of FirstNet PTT users who can communicate with users on an LMR channel. The FirstNet PTT administrator creates an LMR Interop talkgroup and assigns the interoperability profile that corresponds to the correct port on the RoIP gateway/LMR channel. This process associates the groups on both networks and allows FirstNet PTT users to communicate with LMR users.

To help make sure connections are correct, we recommend you name the interoperability profile with the LMR system identifier and channel name you plan to connect to the FirstNet PTT system.

If you delete or suspend an interoperability profile, the LMR connection is immediately deactivated from the FirstNet PTT service. If you change the interoperability profile name or username, a fundamental aspect of the credential changes and the LMR connection is immediately deactivated from FirstNet PTT service.

If the gateway license for an LMR Interop talkgroup is suspended or canceled, the talkgroup becomes dormant and is automatically deleted after 365 days. If the gateway license is reactivated or replaced with a new gateway license, the talkgroup is enabled again. You can't add or edit users in a dormant talkgroup. To delete a dormant talkgroup, be sure to remove all users first.

Create an LMR Interop talkgroup

1. From the dashboard, click **Talkgroup.**
2. Do 1 of the following:
   - If this is your first talkgroup, click **Create.**
   - If you already have talkgroups, click the Plus icon below the list of talkgroups.
3. In the **Create a Talkgroup** window that opens, under **Talkgroup Type**, select **LMR Interop Talkgroup.**
4. For **Network type**, select **On-network.**
5. Enter a talkgroup name using these guidelines:

- Use letters, numbers, and these special characters: [+ @ # $ & ( ) _ , . !]
- If you use spaces, use only in the middle of the name, not as the first or last character
- Use a maximum of 80 characters

6. For the nearest server location, enter the 5-digit ZIP Code where the talkgroup will primarily be used and click **Search.** If the correct location appears, click **OK** to confirm.
7. Select **Normal** or **High priority.**
8. Provide a description up to 200 characters (optional).
9. Click **OK.**

In the Alert notice that appears, click OK to proceed. The talkgroup you created appears in the talkgroup list on the left.

Add the interoperability profile and FirstNet PTT users

Each LMR Interop talkgroup needs an interoperability profile added before any FirstNet PTT users can be added. A gateway license must be assigned to the interoperability profile before it's added to the talkgroup.

Note: You can add up to 5 Interoperability Profiles for each LMR Interop talkgroup.

1. From the dashboard, click **Talkgroup.**
2. From the talkgroup list on the left, select an LMR Interop talkgroup.
3. In the agency tree area to the right, select **Interoperability Profile** and click **Add User.** The user appears in the middle table.
4. Click **Save.**
5. To add FirstNet PTT users to the LMR Interop talkgroup, repeat steps 1-2, and then proceed to step 6.
6. From the agency tree area to the right, select the FirstNet PTT users you want to add and click **Add User.**
7. Click **Save.**

   Note: Make sure to check the FirstNet PTT users also have an LMR Interop Add-on license assigned before you add them to the LMR Interop talkgroup.

Re-enable a dormant LMR Interop talkgroup

Each LMR Interop talkgroup needs at least 1 activated interoperability profile to keep it enabled. If the gateway license for all interoperability profiles in the LMR Interop talkgroup is suspended or canceled, the talkgroup becomes dormant and will be automatically deleted after 365 days.

Enable a dormant talkgroup

Reactivate or replace the suspended or canceled gateway license for at least 1 interoperability profile with a new gateway license.

Test your LMR Interop system

Before you use the LMR Interop functionality in the field, you need to test it.

To get started, you need these things:

- A companion radio
- A donor radio connected to your working RoIP gateway (a mobile base station is preferred over a portable handheld device)
- FirstNet PTT-enabled smartphones assigned to your system
- Users to speak on the radio and phones

Test the system

1. User A speaks into the companion radio while User B listens on the PTT-enabled smartphone.
2. Using FirstNet PTT, user B speaks into the smartphone while User A listens on the companion radio.

Additional information

In this chapter, you'll find additional information about span of control, suspended and canceled licenses, PTT devices, and call prioritization.

Span of control

Span of control refers to the data you can access related to FirstNet PTT. When you log in to the FirstNet PTT Admin Tool, you either have access to all data or to specific foundation accounts or billing accounts only. The data you have access to is your span of control.

As a FirstNet PTT administrator, you can manage users associated with your agency. Your agency is defined by an Org ID, which is a 6-digit alphanumeric code found in your agency's name. The Org ID generally corresponds to your agency's foundation account number. If your agency has several account numbers, your Org ID corresponds with the highest account level.

A FirstNet PTT administrator may be the administrator for multiple accounts. If this is the case for you, you'll manage all of the agency's users under all of those account numbers.

If you have several account numbers under several different Org IDs, you can contact FirstNet Customer Service and request that they be linked at the Org ID level so you can manage the agency's entire user group.

If you're an agency administrator (rather than a super administrator), your span of control is limited to the agencies that you've been assigned to manage.

About suspended or canceled licenses

You can ask your FirstNet representative to suspend or cancel a user's license at any time. After a user's license is suspended or canceled, you need to remove (revoke) the license from the user. You can do this in the FirstNet PTT Admin tool. For information, see Revoke a license.

A suspended or canceled license remains active for a grace period to give you time to revoke the license for the impacted user and notify the user that PTT service isn't available.

The following table shows standard grace periods:

License	License type	Suspension grace period	Cancellation grace period
FirstNet PTT subscription	Single (1:1)	N/A	1 day
FirstNet PTT subscription	Mutiple (PxQ)	3 days	7 days
FirstNet PTT LMR Interop Add-on	Single (1:1)	N/A	1 day
FirstNet PTT LMR Interop Add-on	Multiple (PxQ)	N/A	7 days
FirstNet Gateway	Multiple (PxQ)	7 days	30 days

Table x: Grace period given for each license

About Push-to-Talk devices

FirstNet Push-to-Talk is available on FirstNet certified Android and Apple devices. We maintain a list of certified devices at FirstNet Push-to-Talk Devices, and update the list as new devices become available. Each device in the portfolio is tested and certified for optimal FirstNet PTT service performance. This selection of devices gives you the flexibility to select the devices best suited for your team.

If your device isn't certified and you log in to the FirstNet PTT application, we'll send you a notification letting you know that your device isn't supported.

View user device information When users log in to the mobile app, it sends their device information and wireless number to the PTT Admin Tool.

To view a user's device information:

1. From the dashboard, click **Agency** and select the user you want to view.
2. On the user profile, select **User Device Details**.

Log in to FirstNet PTT on your device

From your certified device, download the FirstNet Push-to-Talk from the App Store® or Google Play®. After you download and install the app, log in to it using your FirstNet ID and password or your federated organization's credentials.

After you've logged in, the application will log off only for the following reasons:

- Application is idle for 7 days

- Device leaves network coverage
- Device is set to flight mode
- Battery runs out

Roam with your device

The FirstNet network is optimized to provide the highest level of network prioritization to FirstNet PTT traffic, excluding mandated emergency calling.

For the best performance, make sure you upgrade your device software and the FirstNet PTT application when updates are available.

Roam domestically

When you're connected to the FirstNet network, the FirstNet logo displays on your device and you'll receive the highest level of prioritization on the network (excluding mandated emergency calling).

When you're not connected to the FirstNet network, Roaming displays as the network provider on your device. FirstNet PTT will continue to work, but you won't have FirstNet PTT standard of network prioritization.

Roam abroad

When roaming abroad, you won't have any network prioritization and AT&T international roaming rates apply.

About the dispatcher consoleFirstNet PTT works with dispatch console systems to support a central dispatch operation. Dispatchers can monitor and control multiple FirstNet PTT talkgroups and have priority access to PTT resources.

Use FirstNet PTT over Wi-Fi

You can use your certified device to make PTT calls over Wi-Fi®. Wi-Fi calls are delivered through an integrated VPN to FirstNet PTT access points. From these access points, the call transmits over the FirstNet network to other FirstNet PTT users. For the best experience and to receive network prioritization, use FirstNet PTT over an LTE connection.

- Android devices prioritize LTE for FirstNet PTT calls and use Wi-Fi if LTE isn't available.
- iOS devices prioritize Wi-Fi for FirstNet PTT calls even if LTE is available.

  Note: FirstNet PTT usage over Wi-Fi receives prioritization only when it reaches the FirstNet network.

Call prioritization

FirstNet PTT prioritizes calls in the following order, with emergency group calls assigned the highest priority. A call that is already in progress will be interrupted by a call with a higher priority.

- Emergency group calls
- High priority group calls
- Normal priority group calls
- Ad hoc group calls
- Private (or 1:1) calls

Glossary

Term	Definition
Agency	Generally refers to a public safety entity or other public safety organization. In the FirstNet PTT Admin Tool, you can create and manage agencies and subagencies to group your FirstNet PTT users. Creating agencies lets you build a departmental hierarchy or structure within your organization.
Agency members	Individuals associated with an agency.
Backhaul	LMR Interop requires a connection, called a backhaul, between the RoIP gateway and the FirstNet PTT node. The backhaul may consist of a wireless data connection or a wireline internet connection (when available).
Companion radio	An LMR radio tuned to the same LMR channel as the donor radio. After the RoIP gateway is implemented, you can use the companion radio to make a call to a handset on FirstNet PTT to test end-to-end connectivity.
CSV file	Comma-separated values file. Frequently used when downloading reports or other data files. You can open it using Microsoft Excel or other applicable software.
CTN	Wireless number.

Term	Definition
Customer premise equipment	Equipment that the customer must deploy, typically at their site, to enable LMR Interop. It includes a RoIP gateway, a donor radio, and requisite cabling.
Donor radio	An LMR radio tuned to an LMR channel. It's connected to the RoIP gateway by a cable.
RoIP Gateway	Customer owned and operated equipment required to convert analog LMR signals to FirstNet PTT service.
Home group	A talkgroup designated by the FirstNet PTT administrator as a FirstNet PTT user's default talkgroup.
Emergency group	A specific talkgroup for urgent situations that's designated by the FirstNet PTT administrator as a FirstNet PTT user's emergency talkgroup.
Interoperability profile	An identifier created in FirstNet Central. It's used to associate a specific port on the RoIP gateway with a specific talkgroup. Also known as a Gateway Credential.
Land Mobile Radio (LMR)	A two-way radio system used by public safety organizations for group or 1:1 communication.
LMR Interop talkgroup	A special type of talkgroup that's required to communicate with LMR channels.
LMR channel	The group of LMR users who can talk to the LMR Interop talkgroup.
Mutual aid request	A request for another agency to make resources available for inclusion in your talkgroups. You can send and receive mutual aid requests.
Org ID	Corresponds to your agency's foundation account number. If your agency has several account numbers, your Org ID corresponds with the highest account level.
Profile template	Describes attributes that can be applied to users in bulk.
RoIP	Radio over Internet Protocol. A technology used by FirstNet PTT to provide interoperability with LMR networks.

Term	Definition
Span of control	The data visible to the FirstNet PTT administrator. Other agencies, FirstNet PTT users, and talkgroups may exist within an organization, but if they're not in the FirstNet PTT administrator's span of control, they won't be visible to the PTT administrator.
Sponsor	A third party employed by your organization to manage an LMR Interop implementation.
Subagencies	Organized groups of FirstNet PTT users that represent hierarchies in a PTT organization.
Talkgroup	A group of users created by a PTT administrator. The users within the group can communicate with each other as a group.