

# RADIUS Client Manual

Control Software for the RADIUS Radio-over-IP Communications Gateway



April, 2024

For RADIUS Software Version 4.20



**DESIGNED AND MANUFACTURED BY**  
**SYSTEMS ENGINEERING TECHNOLOGIES CORPORATION**

ALEXANDRIA, VIRGINIA, USA



For Documentation: <https://www.sytechcorp.com/radiusmoreinfo>

For Client Software: <https://www.sytechcorp.com/radiussoftware>

For Direct Assistance: 703-941-7887. Please reference "Radius Support"

[www.SyTechCorp.com](http://www.SyTechCorp.com)

All rights reserved.



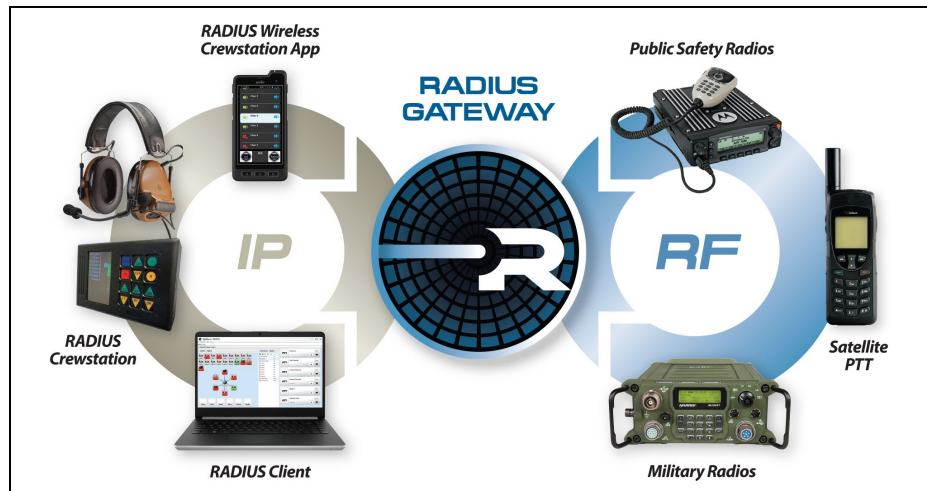
# TABLE OF CONTENTS

<b>1. SYSTEM OVERVIEW</b>	<b>3</b>
<b>2. CLIENT SOFTWARE INSTALLATION</b>	<b>4</b>
2.1 CLIENT REQUIREMENTS	4
2.2 INSTALLING THE RADIUS CLIENT	4
<b>3. RADIUS CLIENT SOFTWARE BASICS</b>	<b>6</b>
3.1 LOGGING IN	6
3.2 SYSTEM OVERVIEW	7
<b>4. RADIUS SYSTEM MODULES</b>	<b>9</b>
<b>4.1 THE ASSETS MODULE</b>	<b>10</b>
4.1.1 LISTENING TO A DEVICE	11
4.1.2 CREATING A PATCH	12
4.1.3 TRANSMITTING TO A PATCH	13
4.1.4 MOVING A PATCH	13
4.1.5 ADDING TO A PATCH	13
4.1.6 RENAMING A PATCH	14
4.1.7 DELETING A PATCH	15
<b>4.2 CHANNELS MODULE</b>	<b>15</b>
4.2.1 VIEWING AND COMMUNICATING TO A CHANNEL	15
4.2.2 CREATING A CHANNEL	15
4.2.3 RENAMING A CHANNEL	16
4.2.4 ADDING TO A CHANNEL	16
4.2.5 REMOVING AND DEVICE FROM A CHANNEL	17
4.2.6 DISABLING AND ENABLING A CHANNEL	17
4.2.7 DELETING A CHANNEL	17
4.2.8 CHANNELS WITH A RADIUS MULTISITE	17
<b>4.3 DASHBOARD MODULE</b>	<b>18</b>
4.3.1 PUSH TO TALK TO A CHANNEL	18
4.3.2 MUTING A CHANNEL	18
4.3.3 VIEW CHANNEL PARTICIPANTS	18
4.3.4 SELECT BUTTON	19
4.3.5 AUDIO PANNING	19
<b>4.4 REMOTE RADIO CONTROL AND THE VIRTUAL CONTROL HEAD</b>	<b>20</b>

<b>5. RADIUS ADMINISTRATION</b>	<b>23</b>
<b>5.1 USER EDITOR</b>	<b>23</b>
5.1.1 CREATING A NEW USER	24
5.1.2 USER PROFILE ASSIGNMENT	24
<b>5.2 USER PROFILE EDITOR</b>	<b>25</b>
5.2.1 CREATING A NEW USER PROFILE	25
5.2.2 LOGGING IN WITH A USER PROFILE	29
<b>5.3 DEVICE EDITOR</b>	<b>30</b>
5.3.1 RADIO DEVICE CONFIGURATION	31
5.3.2 CREW STATION DEVICE CONFIGURATION	33
5.3.3 MOBILE CREW STATION DEVICE CONFIGURATION	35
5.3.4 VOIP DEVICES	36
<b>5.4 MULTISITE AND SITE EDITOR</b>	<b>39</b>
<b>5.5 UPDATING THE RADIUS DS AND CREWSTATION</b>	<b>40</b>
<b>5.6 CHANGING THE EXTERNAL DS IP ADDRESS</b>	<b>41</b>
<b>5.7 RESTARTING THE DS</b>	<b>42</b>
<b>6. MODIFYING THE RADIUS CFG FILE</b>	<b>43</b>
6.1 ACCESSING THE RADIUS CLIENT CFG FILE	43
6.2 SET AUTO LOGON SETTING	43
6.3 SET A PTT TRIGGER DEVICE	43
6.4 VIRTUAL CONTROL HEAD LAYERING	43
6.5 ENABLING TLS ON THE RADIUS CLIENT	44
<b>7. RADIUS MOBILE CREWSTATION APPLICATION</b>	<b>45</b>
7.1 CONNECTING THE MOBILE DEVICE	45
7.2 USING THE MOBILE APP	46
<b>8. RADIUS BOARD CONFIGURATION UTILITY</b>	<b>47</b>
8.1 CHANGE THE IP ADDRESS OF A DEVICE	47
8.2 ADD A NEW DEVICE TO THE RADIUS DS	48
<b>9. COMMON SUPPORT ISSUES AND TROUBLESHOOTING</b>	<b>50</b>

## 1. SYSTEM OVERVIEW

The SyTech Radio and Digital Intercom Unified System (RADIUS) interconnects radios, computers, smartphones, and crewstation intercoms allowing for interoperable voice communications among disparate communications platforms. The system operates via a Linux-based hardware/software configuration that allows system control via network connection and personal computer operating the RADIUS Client.



RADIUS allows end users to communicate via various endpoints operating on analog devices such as two-way radios and IP devices such as computers, smartphones, and the RADIUS crewstation. Together, the system creates a network allowing interoperable communications from various devices. The illustration below depicts a RADIUS system featuring radios, smartphones, computers, and the RADIUS crewstation.

The following document provides an operational outline regarding the software functionality of the RADIUS Software. Please reference the corresponding hardware manual for additional information regarding the specific RADIUS hardware for your system.

For additional questions, please contact SyTech at 703-941-7887.

## 2. CLIENT SOFTWARE INSTALLATION

### 2.1 Client Requirements

The RADIUS Client application allows system users to access the RADIUS network with a Windows personal computer. The prerequisites for the RADIUS Client are:

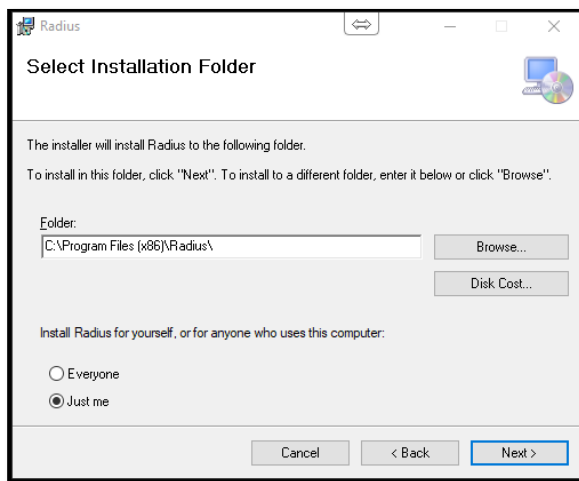
- Windows 10 recommended.
- .NET Framework 4.6+
- Personal computer (PC) connected to the RADIUS Distribution System (DS) Gateway. The RADIUS Client must have two-way IP communications from the PC to the DS.
- The server and client must have **two-way communications** on the required TCP ports.

#### *Quick Tip: RADIUS Port*

- TCP Ports (default): RADIUS Client requires TCP ports 7467 and 7468 for audio receive and transmit. Once the client is connected, a dynamic port within 49,153 – 65,555 will be assigned by the gateway for client communications.
- UDP Ports (alternative to TCP): RADIUS Client requires UPD port 50,000 for audio receive and transmit.

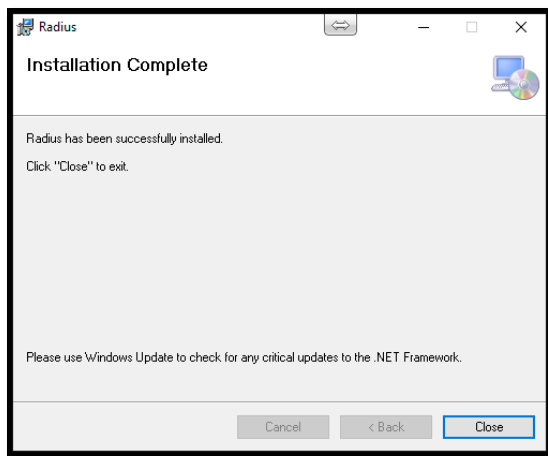
### 2.2 Installing the RADIUS Client

1. Locate and double-click the “Radius Setup” .msi.
2. The Windows Installer will begin.
3. Select the default prompts.



4. The RADIUS Client will be installed.





5. Close the Installation program when complete.
6. The RADIUS icon will be shown on the Window's Desktop.

### 3. RADIUS CLIENT SOFTWARE BASICS

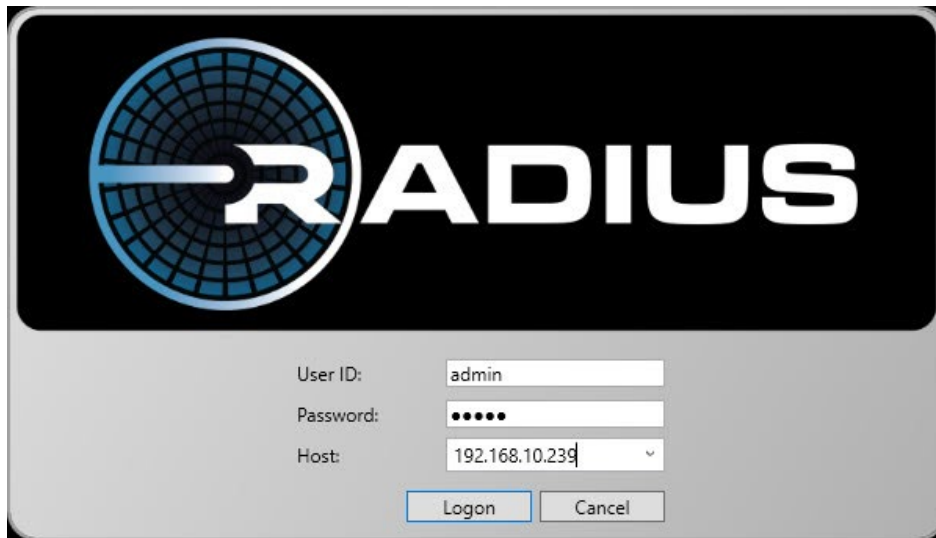
The following section provides an overview of how to access the RADIUS client and the basics of the graphical user interface.

#### 3.1 Logging In

1. Log into RADIUS by double-clicking the RADIUS icon located on the PC desktop.



2. The RADIUS Log In will be displayed as shown below.



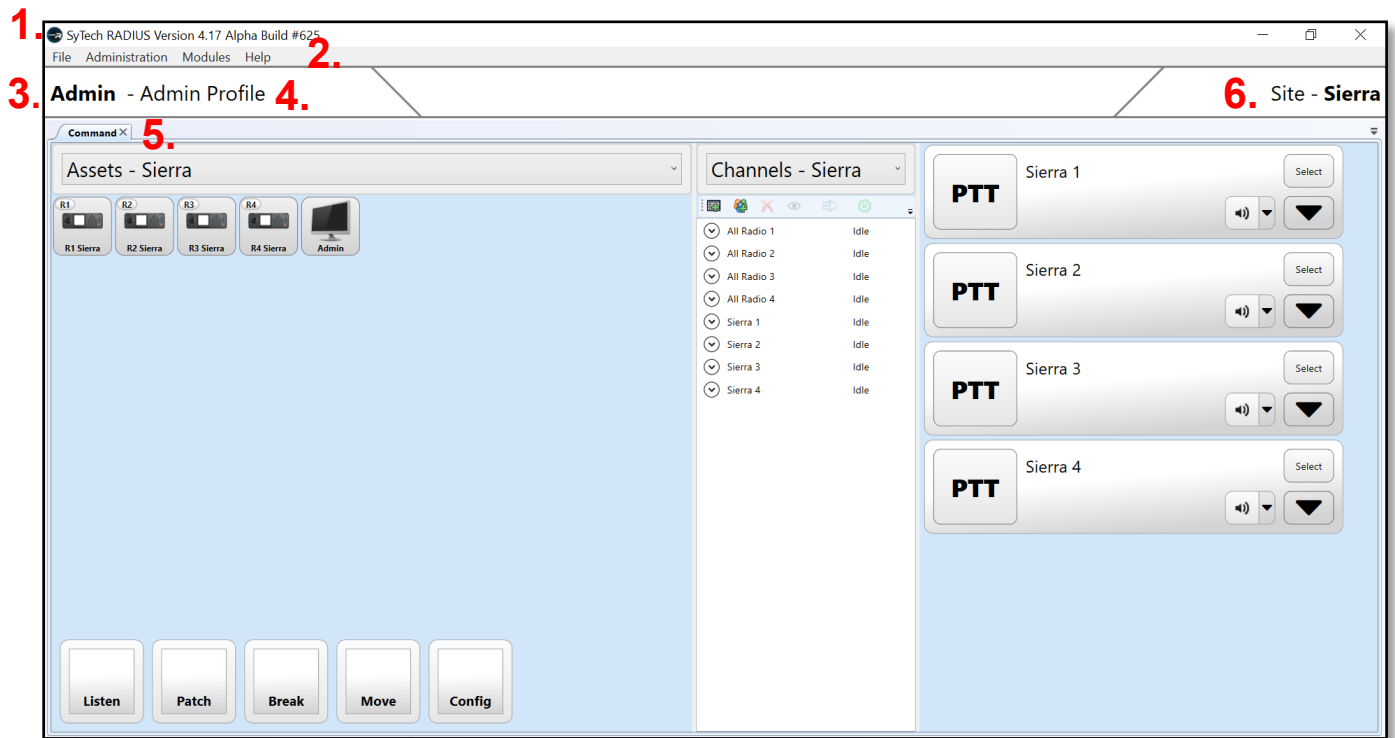
3. By default, the User ID is “**admin**” with a password of “**admin.**”
4. Select “Logon” to log in to the client. The RADIUS Client application will be displayed as shown in the following section.
5. In the “Host” field, input the IP address of the RADIUS server. This will be indicated on the gateway’s LCD screen as “IP Address.”
6. Select Logon.
7. If no additional User Profiles have been assigned, RADIUS will automatically log the user into their profile. If one or more alternative User Profiles have been assigned to the User, select the appropriate User Profile. See Section 5.2 for more information on User Profiles.

### 3.2 System Overview

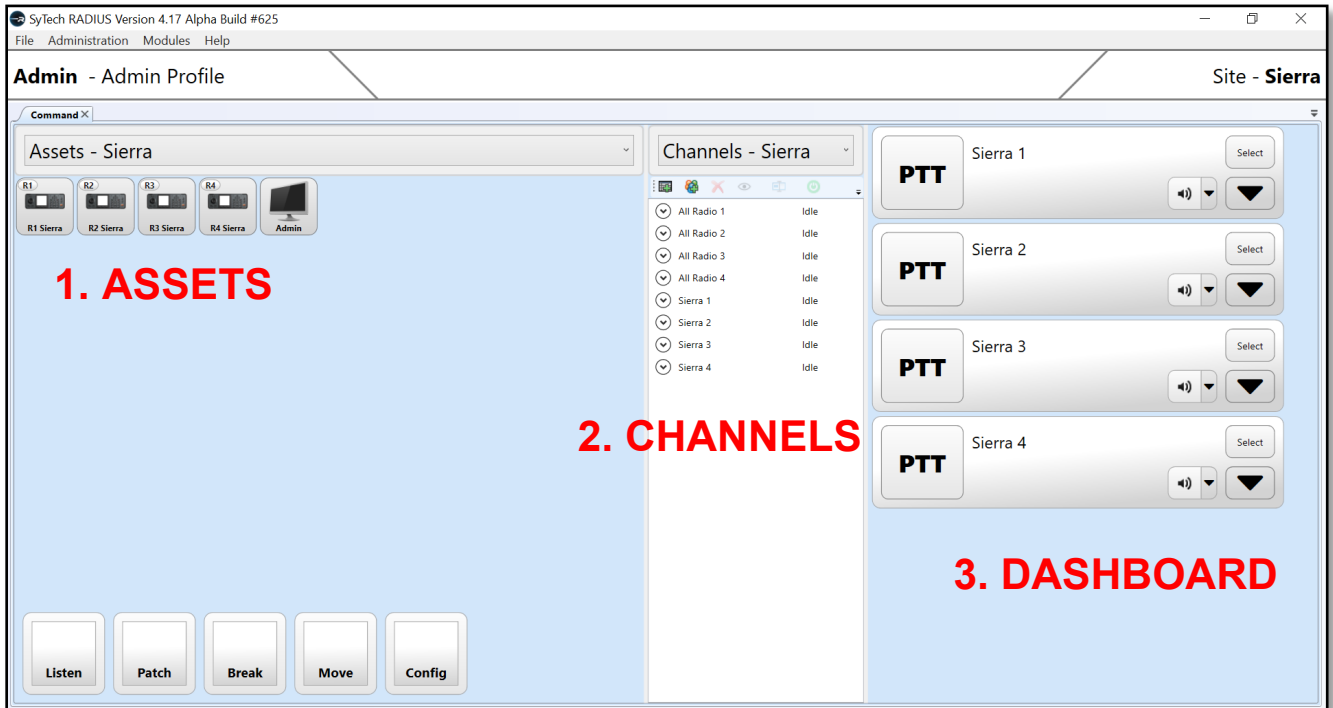
The RADIUS Client combines the functionality of the system administration tool with the capability of the end user control software. By configuring the system for a variety of uses, the system administrator can configure the graphical user interface to meet the needs of a variety of end-user requirements.

The image below highlights the access and log-on information of the RADIUS Client. From top to bottom, these elements are:

1. The application title bar. The RADIUS Client Version is indicated.
2. **The Menu Bar** is presented. The Menu Bar contains a variety of high-level commands for system usage. For example, the RADIUS Administration and Module selection can be found in the File Menu.
3. **The Display Name** of the logged-on user is shown.
4. **The Log-On Profile.** The permissions profile the user is logged on with.
5. **The Command Tab:** The Command Tab contains the active modules currently available to the user. If additional modules are open their tabs will appear in this section.
6. **The Log-on Site:** The name of the site the user is logged into.



RADIUS provides a variety of system tools to communicate, patch, control, and interact with connected assets such as radios, computers, smartphones, and crewstations. The image below displays the basic graphical user interface (GUI) presented to the user.



By default, the RADIUS GUI screen is composed of three interrelated modules. From left to right:

1. **The Assets Module:** Allows the administrator to view and modify specific **assets** available to the system. Assets include **devices** such as crew stations, radios, computers, and crewstations as well as **functions** such as monitor, patch, and control. The user can create patches among assets as well as operate other high-level functions within RADIUS.
2. **The Channels Module:** Allows the administrator to create and modify channels. A **channel** is an administrator-created grouping of assets that can be made available to the end user. The purpose of a channel is to simplify push-to-talk functionality made available to the end user.
3. **The Dashboard Module:** Allows the end user to easily access the channels created by the administrator.

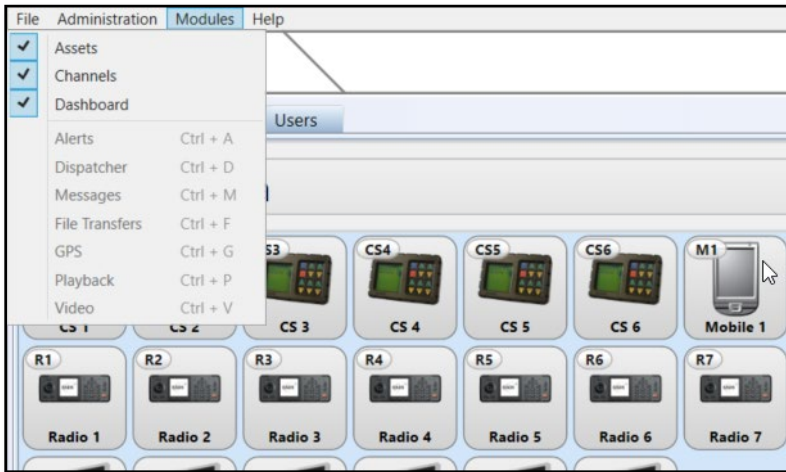
*Quick Tip:* The user can zoom in and out to re-size the graphical user interface using “CTRL + scroll” on a keyboard and mouse or pinch in and pinch out on a laptop touchpad.

Additionally, the user can drag the vertical lines separating the Assets, Channels, and Dashboard to reshape the wrap of the module elements.

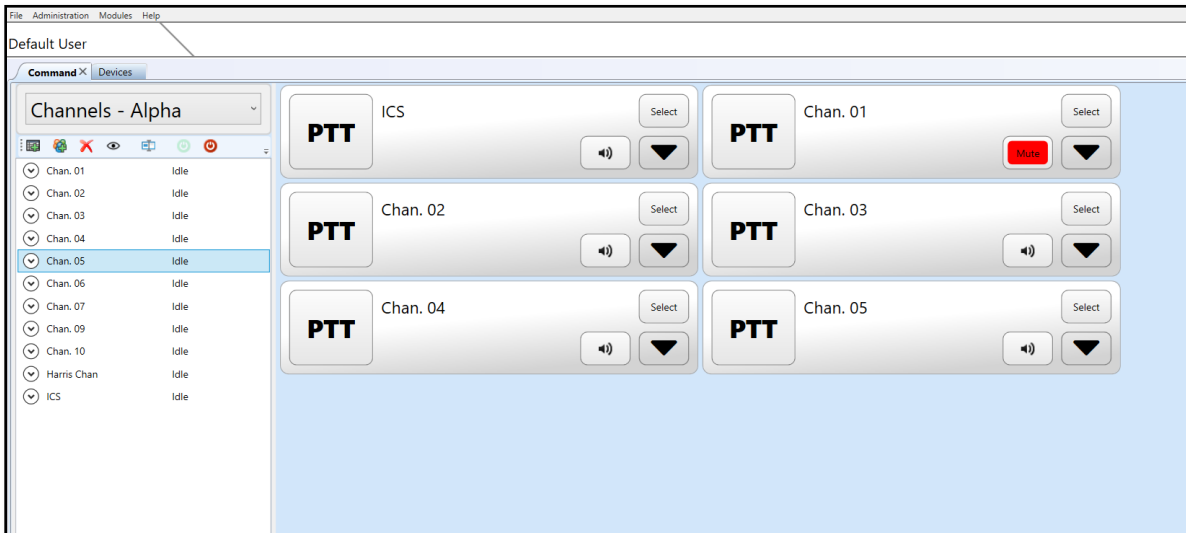
#### 4. RADIUS SYSTEM MODULES

RADIUS System Modules refer to the modular capabilities available to the user. By default, RADIUS features the three core modules of Assets, Channels, and the Dashboard.

From the Menu Bar, select the “Modules” selection as shown below. The dropdown menu will reveal the selected modules with a check mark, available modules in black text, and unlicensed modules in gray text. If the system is licensed for the module and the user is permitted to access the module, the user will be able to select the module.



In the image below, the Assets Module is deactivated, only the Channel and the Dashboard are utilized.



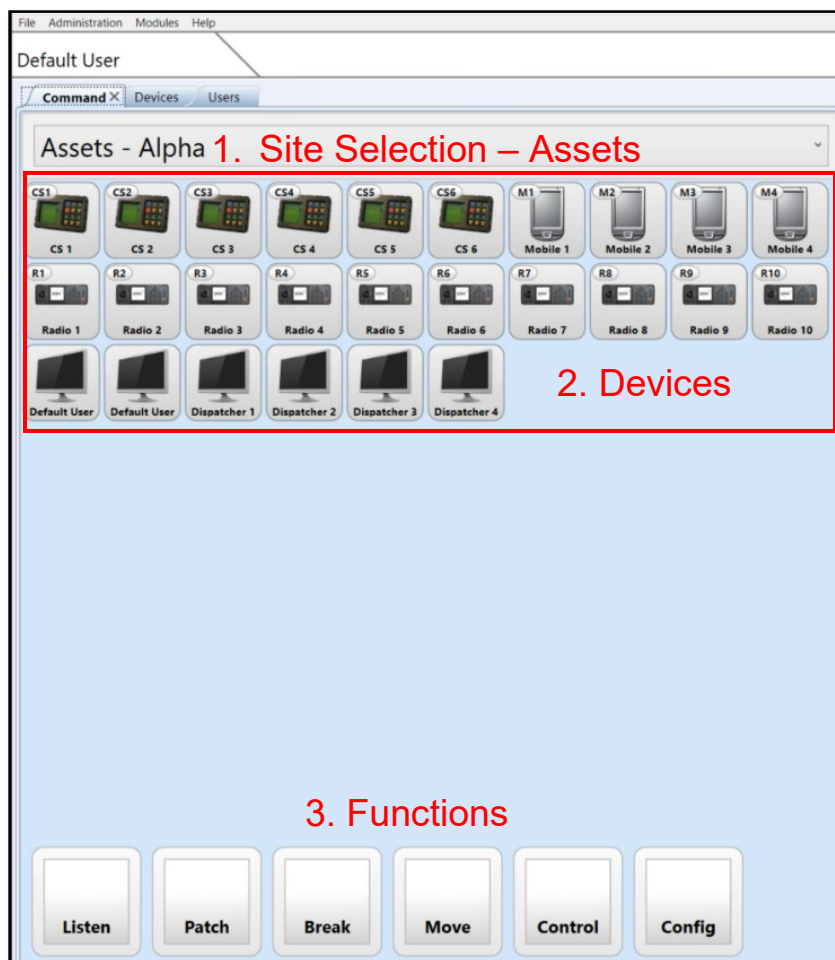
The following section outlines the capabilities and operation of the various RADIUS modules.

## 4.1 The Assets Module

The Assets Module graphically represents the available devices and functions available to the user. If permitted, the user can perform specific operations such as listening to a radio, creating patches among devices, control devices, and other functions.

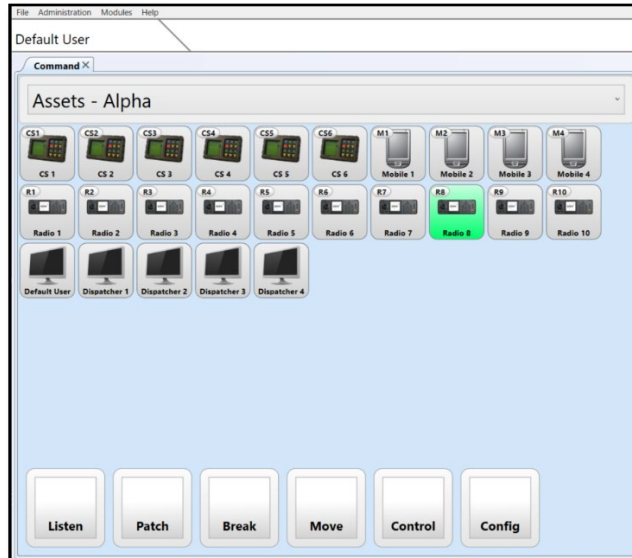
The image below displays the critical elements of the Assets Module:

1. **Site Selection Tool – Assets:** Indicates the user’s selected site to access devices. Used for RADIUS MultiSite when RADIUS systems are connected via an IP network.
2. **Devices:** Graphical representations of the devices licensed for the RADIUS site.
3. **Functions:** Device actions available to the user. If the user is not permitted for the function the corresponding function button will not be shown.



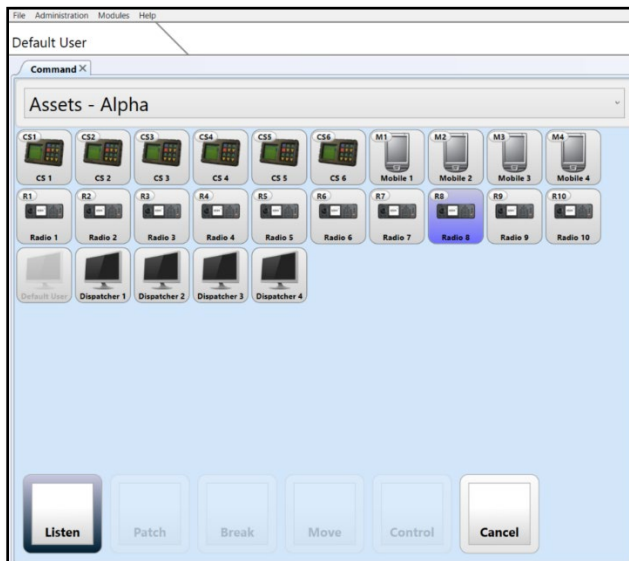
### 4.1.1 Listening to a Device

Listening to a receiving radio may be accomplished using the Listen function and selecting the desired radio to monitor. In the image below, Radio 8 is receiving audio as indicated by the green highlight. It's important to note that the green highlight is an important indicator for receiving audio.



To listen to the receiving radio:

1. Select the Listen function.
2. Select the radio or radios you would like to listen to.

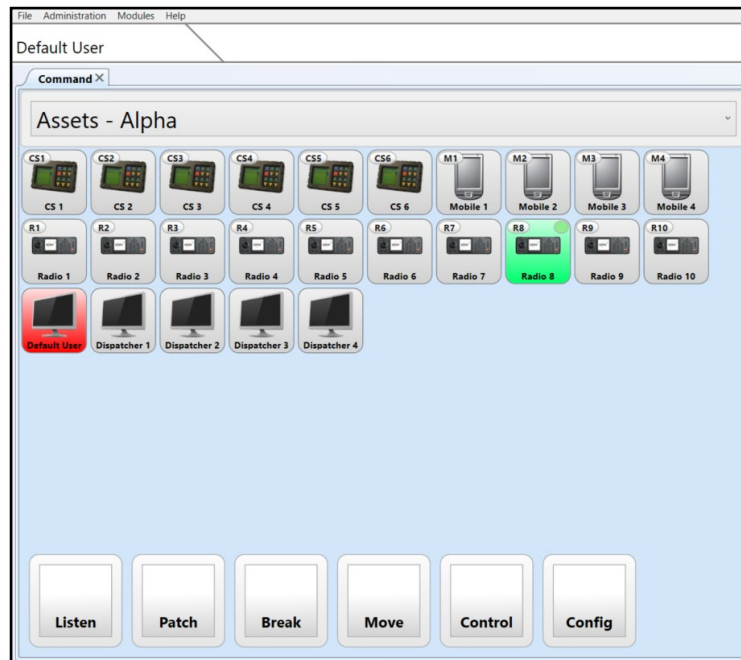


3. Confirm the selection by deselecting the Listen function.

The device will display a green dot at the top of the icon to indicate that it is set to Listen. When audio is received on Radio 8 and transmitted to the Default User, the computer device representing the user turns red to indicate that it is transmitting audio. The image below illustrates the reception (green) and transmission (red). It is important to understand the meaning and orientation of the color code:

**Green: The connected device is receiving audio into it.**

**Red: The connected device is transmitting audio out of it.**



To unmonitor the device, repeat the logic above to deselect it.

#### 4.1.2 **Creating a Patch**

RADIUS allows system users to create crossbanded patches or nets among disparate radios and end-user devices.

To create a patch:

1. Select the Patch function within the Command Module. The unavailable functions will become transparent.
2. Select the assets that are to be patched together.
3. Finalize the patch by re-selecting the Patch function.

The patch will be shown onscreen as a RADIUS patch. The patch will also be shown within the Channels interface as a "new patch."

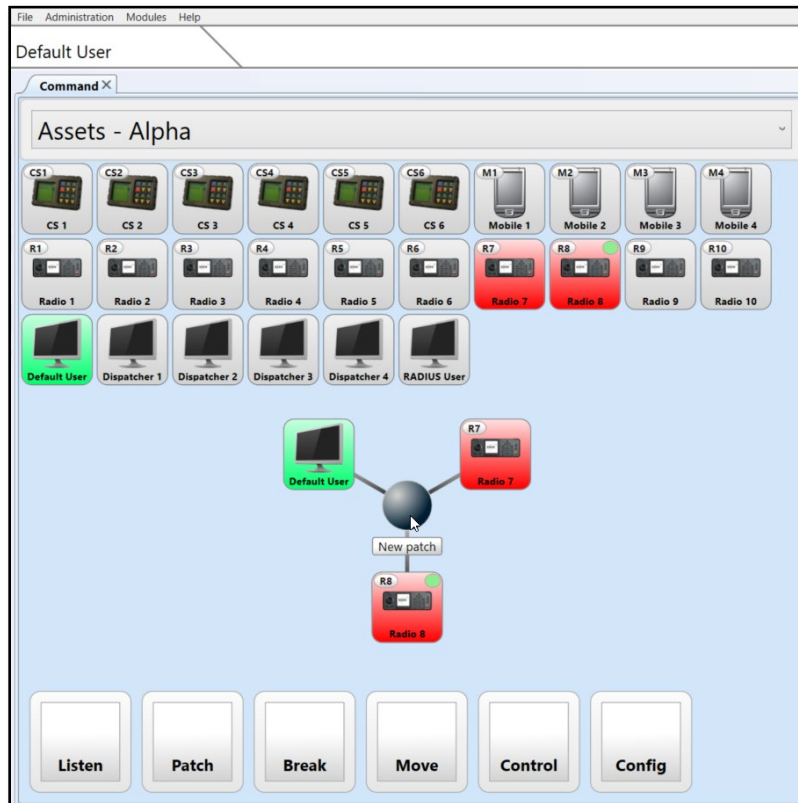


To remove the patch, select the Break function followed by selecting the center node of the patch, and then confirming the break by reselecting the Break function.

#### 4.1.3 **Transmitting to a Patch**

To transmit to a patch, press the center node of the patch.

Your logged-on device will automatically join the patch as shown below. The radios in the patch will turn red to indicate transmissions. Your device will turn green to indicate it is receiving audio.



#### 4.1.4 **Moving a Patch**

To move a patch:

1. Select the Move function.
2. Select the patch you wish to move and drag it to the new location.
3. Deselect the Move function

#### 4.1.5 **Adding to a Patch**

To add to a patch:

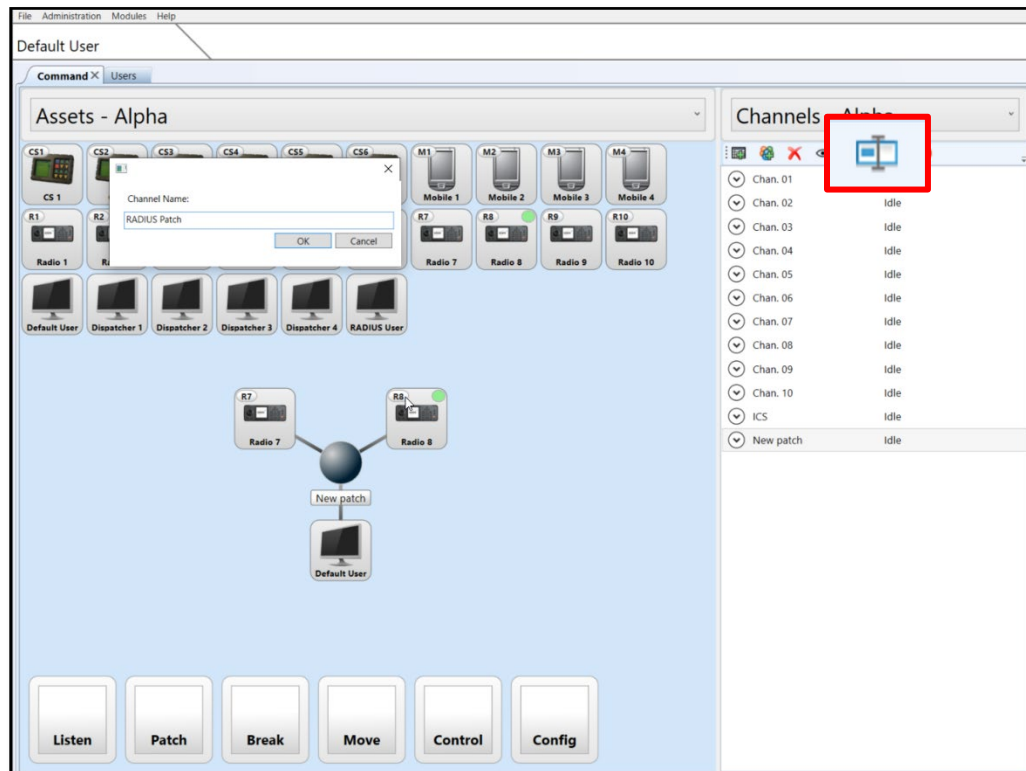
1. Select the Patch function
2. Select the patch you wish to add to. The node of the patch will turn bright blue.
3. Select the devices you wish to add.
4. Confirm the addition by re-select the Patch function. The devices will be added.

#### 4.1.6 Renaming a Patch

Renaming the patch can be accomplished by utilizing the Channels Module. When a patch is created, it is automatically added to the Channel Module.

To rename a patch:

1. Select the patch within the Channels Module. By default, a patch is labeled as “New patch.”
2. Select the Rename icon located in the Channel Tool Bar. The Rename prompt will appear as shown below.
3. Input the patch’s new name and select “OK.”



The center node of the patch will be updated with the new patch name. The new patch name will be alphabetized within the Channel Module.

#### 4.1.7 **Deleting a Patch**

To delete a patch:

1. Select the Break function
2. Select the center node of the patch.
3. Confirm the deletion by re-selecting the Break function.

To remove an individual device, follow the above procedure, choosing the devices you wish to remove instead of the center node.

## 4.2 **Channels Module**

The Channels Module allows the administrator to view, create, and modify the system **channels** within RADIUS. Channels are semi-permeant nets created by the administrator. Channels may include any type of device as well as multiple radios. Devices within a channel can communicate as a group regardless of device type.

There is no limit to the number of channels that can be created within the system. Radios may be placed into multiple channels however it might be good practice to create a channel for each radio asset.

Additionally, it is recommended that the ICS channel remain if crewstations are used for the system configuration. The ICS channel refers to the “intercom system,” a set-aside channel that may be used for internal communications.

There is no limit to the number of channels that can be created. If permissioned, any device can be added to a channel. The device may exist in multiple channels at one time.

#### 4.2.1 **Viewing and Communicating to a Channel**

Double-click on the channel within the channel list to view a channel, and the channel will appear in the Dashboard. If permissioned the user can communicate through the channel from within the Dashboard.

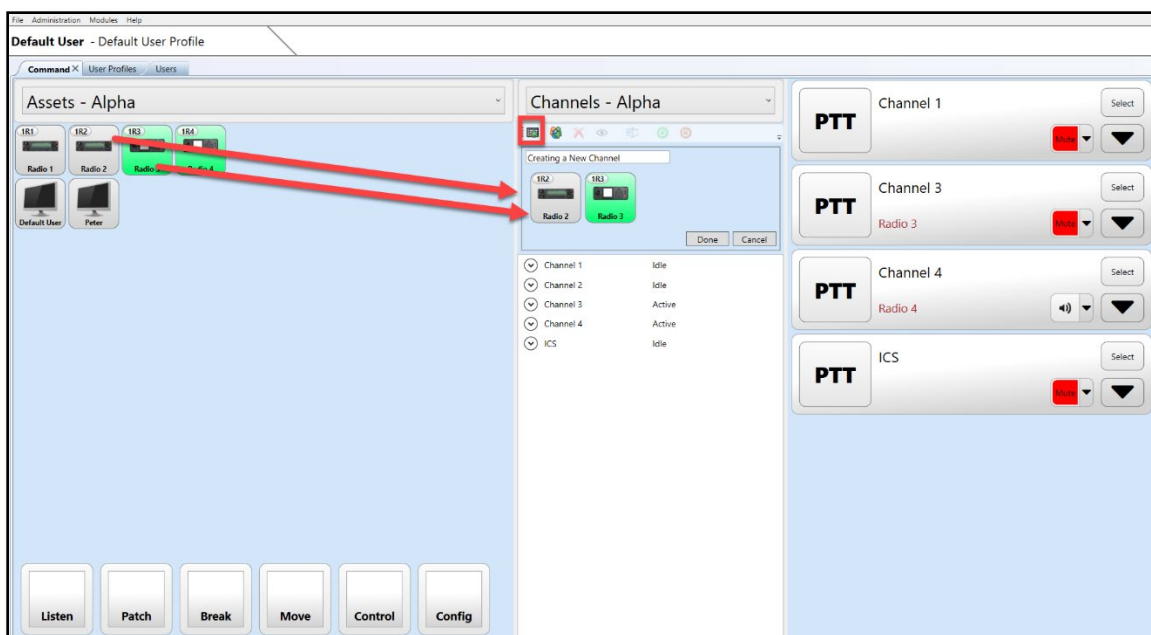
The “Show” icon may also be used to view the channel within the Dashboard.

Reversing the process above will hide the channel. When the channel is removed from the Dashboard it is automatically muted.

#### 4.2.2 **Creating a Channel**

To create a new channel:

1. Select the “New Channel” icon.
2. Drag and drop the desired assets into the channel creation area.



3. Input the desired name of the new channel.
4. Select “Okay” to complete the new channel.
5. The new channel will be shown. Channels are alphabetized within the list. The user can view the channel by double-clicking on the channel to access it from the Dashboard.

#### 4.2.3 **Renaming a Channel**

To rename a channel:

1. Select the “Rename” icon found within the Channel Tool Bar.
2. Input the new name of the channel

#### 4.2.4 **Adding to a Channel**

To view channel members, the user can select the dropdown icon adjacent to the corresponding channel.

To add devices to a channel:

1. Select the dropdown menu adjacent to the channel.

2. Drag and drop the device from the Assets module to the channel to receive the new device.
3. Select “Ok.”

#### 4.2.5 **Removing and Device from a Channel**

To remove a device from a channel:

1. Locate the channel within the Dashboard.
2. Select the Dropdown icon from within the channel.
3. Select the device you would like to remove.
4. Select the “Remove” icon found within the channels Dashboard Tool Bar.

#### 4.2.6 **Disabling and Enabling a Channel**

To disable a channel:

1. Select the channel from the channels list.
2. Select the “Disable” icon found within the Channels Tool Bar.
3. The channel will

#### 4.2.7 **Deleting a Channel**

To delete a channel:

1. Select the channel from the channels list.
2. Select the “Remove” icon from the Channels Tool Bar.

#### 4.2.8 **Channels with a Radius Multisite**

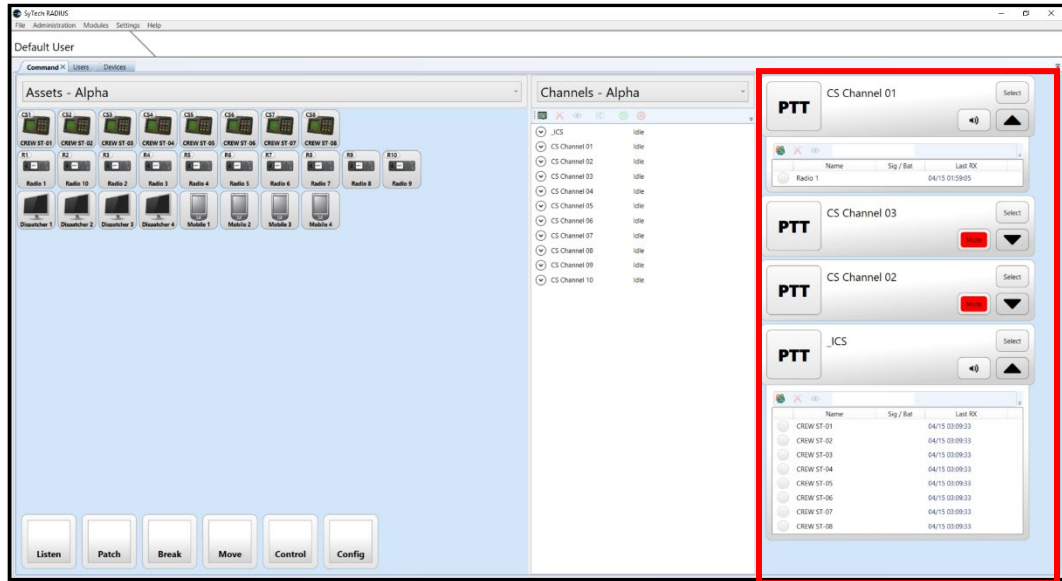
For Radius systems within a multisite configuration, Channels operate with similar rules compared to a single site. One difference of note is that if a remote operator adds a local asset to the remote channel, the channel will appear in both the remote and local channel lists.

If the remote site is offline, the operator will not be able to delete the remote channel from within the Radius client application.

### 4.3 Dashboard Module

The Dashboard Module allows the end user to easily access the channels created by the administrator.

From within the Dashboard, the end user can Mute, Unmute, PTT, Select, and view who is associated with the Channel.



#### 4.3.1 Push to Talk to a Channel

Press the PTT button on the channel to push-to-talk to the channel. The PTT button will illuminate in green to indicate that it is receiving audio.

When receiving on the channel, the originator of the audio will be displayed below the channel name.

#### 4.3.2 Muting a Channel

To mute or unmute the channel, toggle the “Mute” button on the channel. The user can also double-click on the channel from the Channels Module to hide and mute the channel.

#### 4.3.3 View Channel Participants

To view channel participants, select the dropdown area on the channel. A list of the channel participants can be seen. For this location, permissioned users can add or remove channel participants.

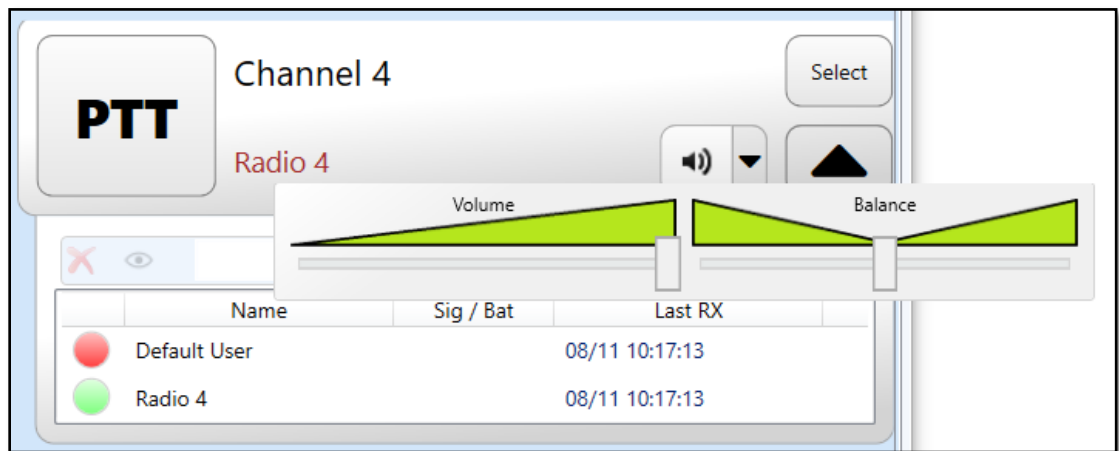
A green or red indicator will be illuminated adjacent to the respective participant when receiving or transmitting audio within the channel.

#### 4.3.4 **Select Button**

The “Select” button enables the users to select which channel will receive audio when a push-to-talk device is used in conjunction with RADIUS. By default, **the user can use the keyboard for selective push-to-talk by pressing “CTRL” and the spacebar.**

#### 4.3.5 **Audio Panning**

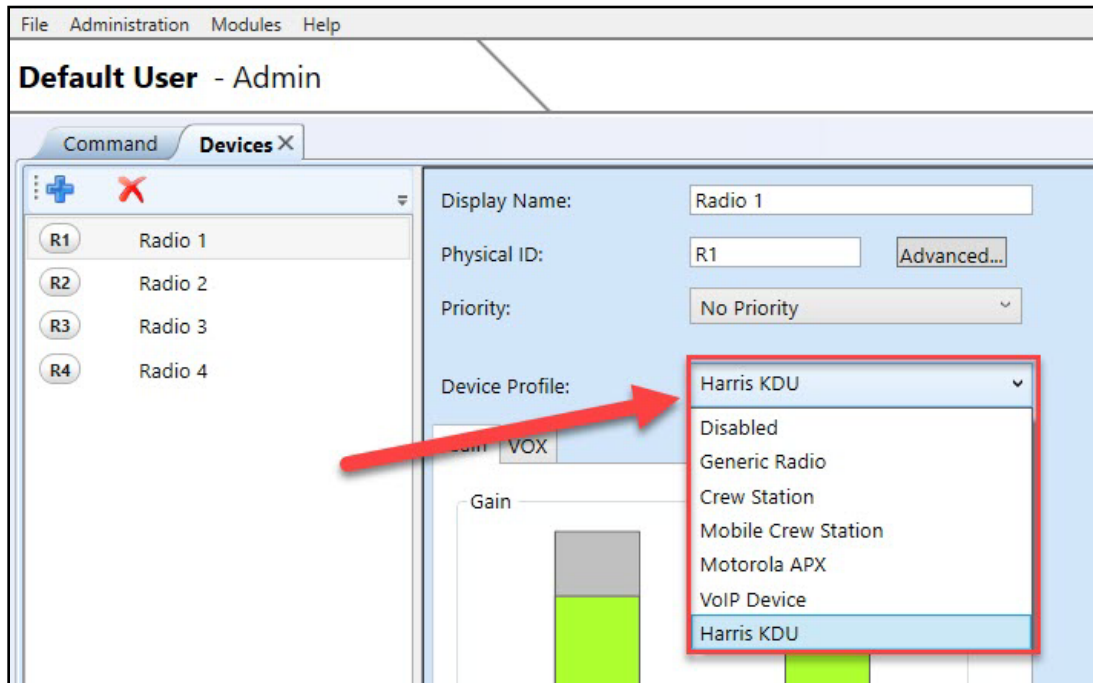
The Audio Panning feature within the Dashboard channel allows the user to control the audio level from the channel as well as control the left/right audio balance of the audio. To access the audio panning control, select the drop-down arrow located next to the mute/unmute button on the channel. The audio panning control will be visible as shown below.



#### 4.4 Remote Radio Control and the Virtual Control Head

RADIUS offers the ability to remotely control a variety of radio models. Popular radio models include the Motorola APX O5 and E5 control heads as well as several models of the Harris military radios via remote KDU port.

If licensed, the administrator can load the applicable radio profile within the Device Editor. In the image below, the Harris KDU profile is selected for Radio 1.



Once the profile is loaded for the corresponding radio, the operator can access the Virtual Control Head (VCH) from within the Assets module.

##### To Remotely Control a Radio

1. Select "CONTROL."
2. Pick the Asset. The corresponding VCH will be shown.

In the image on the following page, a VCH for the Harris KDU is made accessible. The controls for the KDU VCH are labeled on the image and described below.

**Display Name:** The name as indicated in "Display Name" is found within the Device Editor.

**Display Screen:** The information sent from the radio will be shown here.

**Push to Talk:** Allows the user to PTT to the radio. When engaged, the PTT button will light up green (the KDU is receiving audio). When the radio is *receiving* audio the KDU



will light up red (the KDU is emitting audio). After a reception, the PTT button will flash yellow for five seconds.

**Audio Control:** Allows the user to mute and pan the audio level and balance. Note that when the control head is first opened, its default setting is muted. When a PTT occurs, the VCH will automatically unmute.

**Memory Toggle:** Enables the VCH to appear as it appeared when the client program was previously closed. Toggling the memory toggle will save the VCH's size and location for when the RADIUS client is re-opened.

**PTT Select:** Engages a PTT button such as a hardware PTT button or the keyboard using CTRL + Spacebar. The VCH must be unmuted for the PTT Select to be engaged.

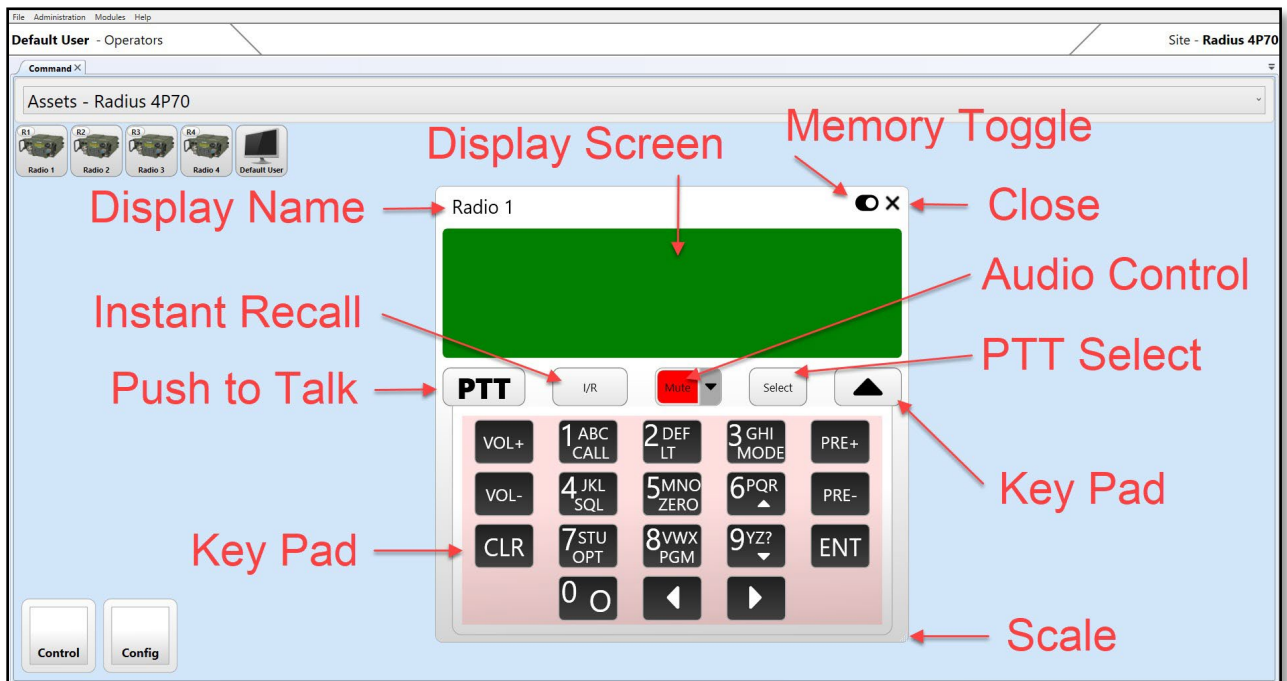
**Keypad:** Provides the available button controls to the user. When the keypad appears pink, RADIUS does not sense the radio. When the radio is correctly connected, the keypad will turn light gray. The pink background color indicates that the radio is not communicating with the gateway

**Keypad Control:** Opens and closes the keypad.

**Instant Recall:** Plays back the last audio reception (if licensed and permissioned).

**Scale:** Allows the user to rescale the VCH.

**Close:** Closes the VCH.



---

Layering: The user can set the VCHs to layer over to all other windows on the local computer. To enable the “TopMost” setting, see section 6.4, *Virtual Control Head Layering*.

Remote Radio Control Cables: RADIUS requires the corresponding RIOS Interface Cables for remote control capability. Popular radio and cables include:

Motorola O5 and E5: CAB-00209B

Harris 117G: CAB-00272 (with RS-232 RIB default, with RS-485 RIB use CAB-00271)

Harris 160: CAB-00271

Harris 163/167: CAB-00273

## 5. RADIUS ADMINISTRATION

The RADIUS Administration tab allows the administrator to control the admin functions of the systems. These functions include creating User IDs and Profiles, modifying device configurations, updating the system software, and loading and saving system presets.

The major portions of the Administration tab include:

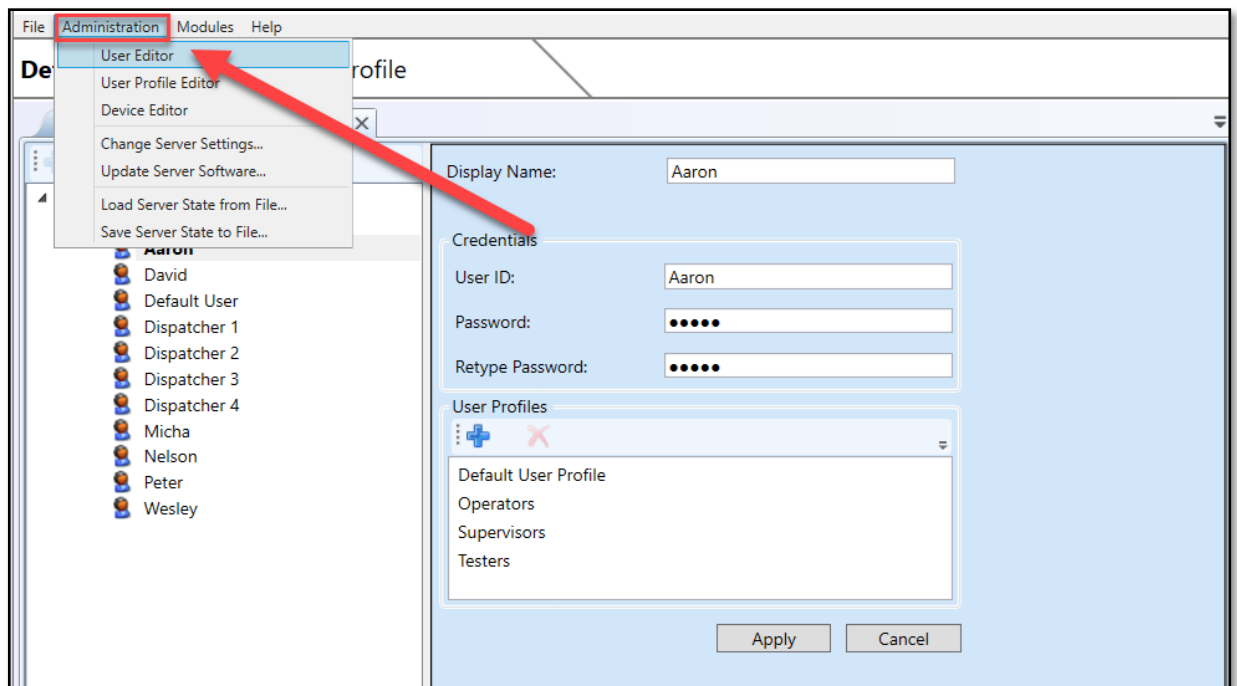
- **User Editor:** Allows the administrator to create user names and passwords and assign the users to User Profiles.
- **User Profiles:** Allows the administrator to create User Profiles. User Profiles can be thought of as “access templates” for user groups.
- **Device Editor:** Allows the administrator to modify and add devices such as radios, crew stations, and mobile crew stations.
- **Site Editor:** Allows the administrator to add, delete, or modify the IP connections to RADIUS Gateways connected in a RADIUS MultiSite.

The following sections outline the Radius Administration control as well as highlight other capabilities found within the Administration tab.

### 5.1 User Editor

The RADIUS User Editor allows the administrator to create users and user credentials. To access the “User Editor” select it from the Administration tab.

The RADIUS User Editor will be shown as displayed below.



### 5.1.1 Creating a New User

To create a new user:

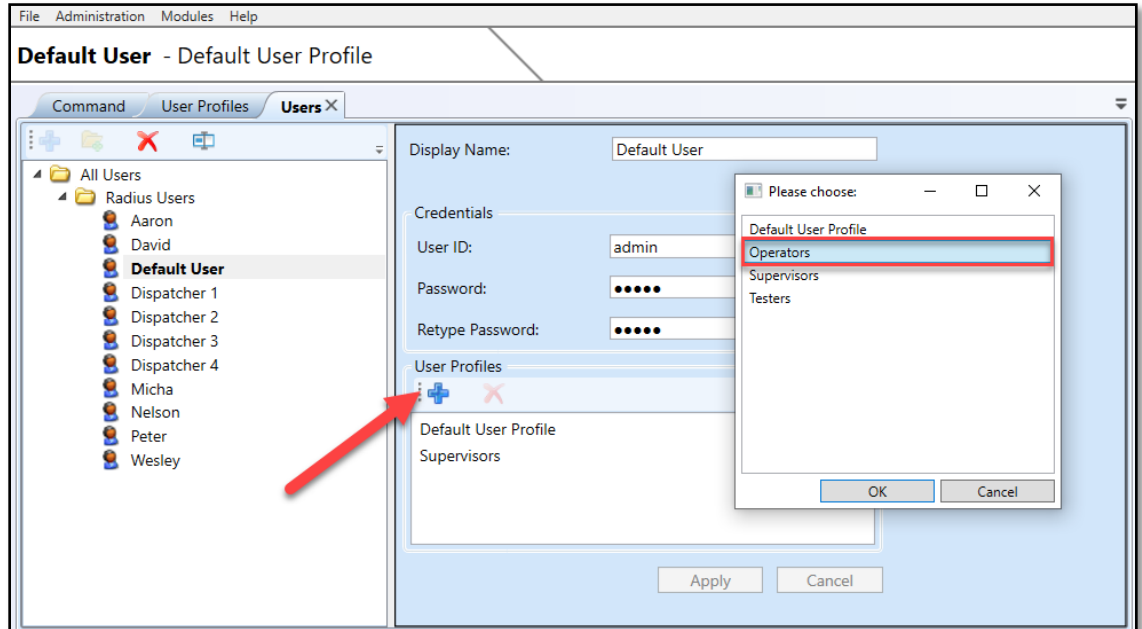
1. Select the group where the new user will reside.
2. Select the “+” icons to create the new user.
3. Input the desired Display Name, User ID, and password.
4. Select “Apply.”

### 5.1.2 User Profile Assignment

Access to resources and system capabilities are defined by the User Profile. The following section titled “User Profile Editor” outlines how to create User Profiles. If User Profiles are already created, the administrator can assign the users to the User Profile within the User Edit.

The administrator can assign the appropriate User Profiles within the User Edit.

The image below shows the administrator adding a User Profile to the “Default User.” To add a User Profile, select the “+” and the available profiles will appear. Select the desired profiles and select “OK” and “Apply.”

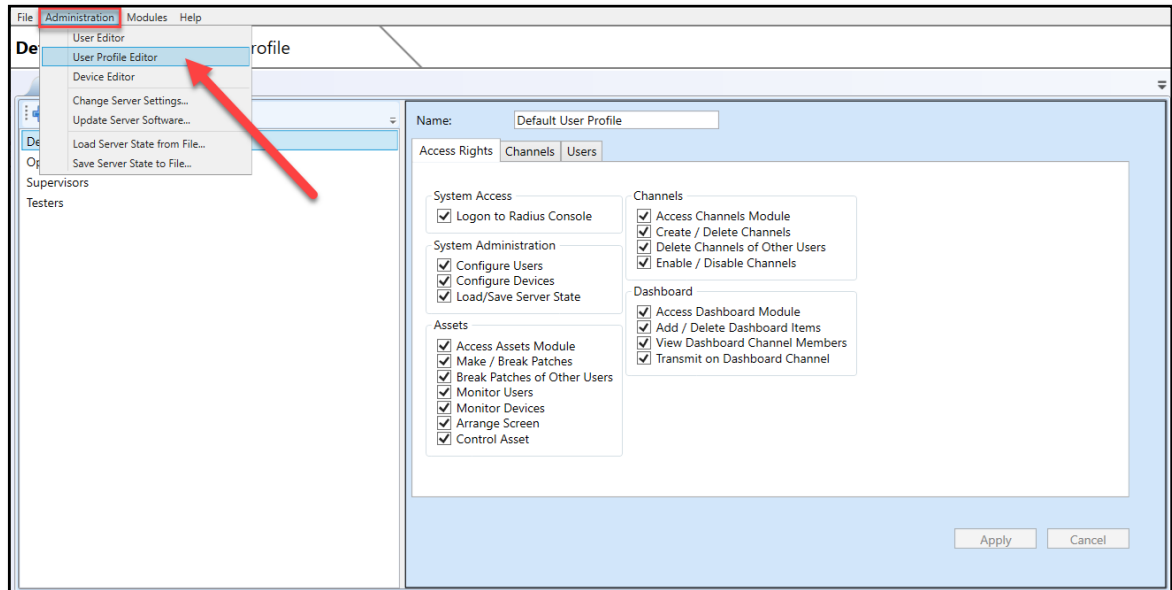


When the Default User logs in next time, the user will have the option to select the desired profile for login. User Profiles are covered in more detail in the following section.

## 5.2 User Profile Editor

The User Profile Editor allows the administrator to determine access rights and channel availability to users added to the profile. User Profiles function as “access templates” to user groups as created by the administrator. For example, in the image below the administrator has created three additional User Profiles in addition to the “Default User Profile.” Created User Profiles in this example include “Operators,” “Supervisors,” and “Testers.”

Note: The “Default User Profile” functions as the default administrator user. The administrator may change the name of this profile but it can not be deleted.



Within the User Profile Editor, the following tabs provide access control for the selected User Profile:

- Access Rights: Determines the capabilities available to the users within the User Profile
- Channels: Determines which channels are available to the users within the User Profile
- Users: Determines which users will be members of the User Profile

### 5.2.1 Creating a New User Profile

To create a User Profile:

1. Select the “Add User Profile” as indicated with the blue “+” sign located in the top left corner.
2. In the list of profiles, a “new user profile” will be shown.

3. Within the “Name” field provide a new name for the User Profile.
4. Within the “Access Right” tab, select the access rights that should be available to the User Profile. The image above illustrates the available access permissions. These rights include:

System Access:

**Login to Radius Console:** Allows the User Profile to log in with the Radius Client Application.

**System Administration:** If the access rights below are disabled the user will not see the corresponding selection within the “Administrator” menu.

**Configure Users:** Allows the User Profile to access the “User Editor” and “User Profile Editor”

**Configure Devices:** Allows the User Profile to access “Device Editor.”

**Load/Save Server State:** Allows the User Profile to access “Load Server State from File” and “Save Server State to File.”

**Assets:** If the access right below is disabled the user will not see the corresponding function within the “Assets” module.

**Access Assets Module:** Allows the User Profile to access the Assets module. If this right is not enabled the user will be able to view any of the assets or functions within the Assets module.

**Make / Break Patches:** Allows the User Profile to access the “Patch” function.

**Break Patches of Other Users:** Allows the User Profile to access the “Break” function.

**Monitor Users:** Allows the User Profile to monitor User devices such as smartphones and computers via the “Monitor” function.

**Monitor Devices:** Allows the User Profile to monitor Assets devices such as radios via the “Monitor” function.

**Arrange Screen:** Allows the User Profile to access the “Move” function.

**Control Asset:** Allows the User Profile to access the “Control” function for Remote Radio Control capability when licensed.

Channels:

**Access Channels Module:** Allows the User Profile to access the Channels module. If this right is not enabled the user will be able to view any of the channels or functions within the Channels module.

**Create / Delete Channels:** Allows the User Profile to create and delete channels.

**Delete Channels of Other Users:** Allows the User Profile to delete channels created by other users.

**Enable / Disable Channels:** Allows the User Profile to utilize the “Enable” and “Disable” functions found within the Channels menu.

Dashboard:

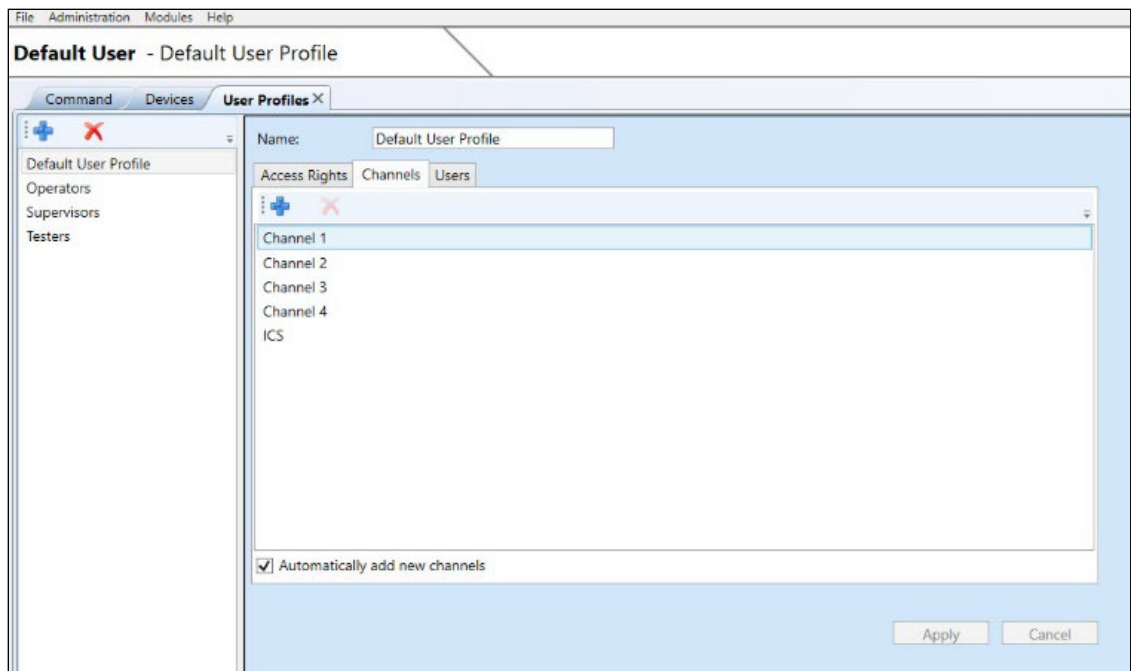
**Access Dashboard Module:** Allows the User Profile to access the Dashboard module. If this right is not enabled the user will be able to view any of the channels or channel controls within the Dashboard module.

**Add / Delete Dashboard Items:** Allows the User Profile to add and remove items from the Dashboard by double-clicking the channels from the Channels module.

**View Dashboard Channel Members:** Allows the User Profile to select the Channel Dropdown to reveal users and assets within the channel.

**Transmit on Dashboard Channels:** Allows the User Profile to transmit on the channel. If this access right is disabled the PTT button on the channel will not be available.

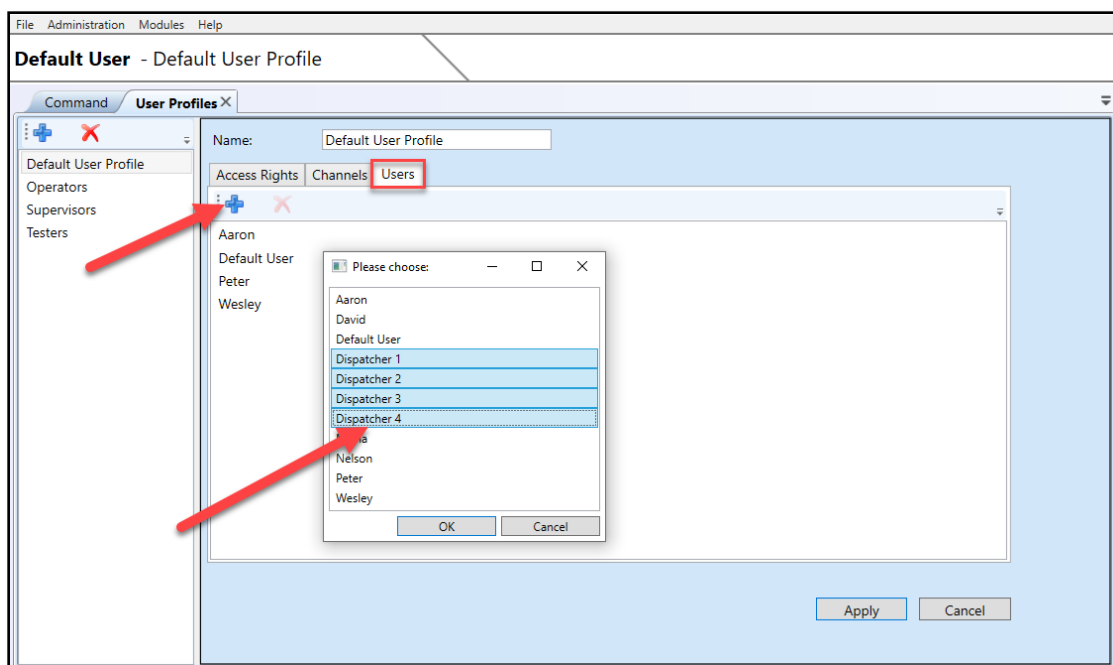
5. Next, select the “Channels” tab. The channels currently assigned to the User Profile are shown. In the example below, Channels 1 – 4 and the ICS Channel are included in the “Default” User Profile.
6. To add or remove channels from the profile, select the blue “+” to add channels or select the existing channel or channels to be deleted and select the red “x.”



Note: The access right titled “Automatically add new channels” allows users within the User Profile to view newly created channels and patches without having to add the channel or patch after it is created. The default is enabled.

7. Next, select the “Users” tab. Users that have access to the User Profile are shown.
8. To add users, select the blue “+” sign. Users created from within the User Editor will be shown. Select the new users to add to the User Profile. Hold CTRL to select multiple users as shown in the image below.
9. Select “Okay.” The users will be added to the User Profile. When the user logs in using the corresponding Username and Password, the user will be able to select the desired profile.





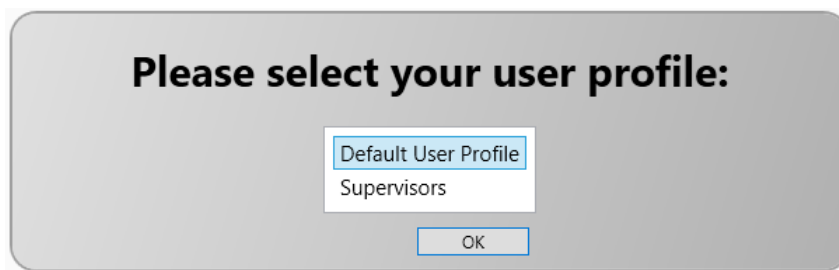
10. Select the “Apply” button.

The User Profile is now created. The corresponding rights, channels, and users will now be enforced by the User Profile.

### 5.2.2 Logging in with a User Profile

If the user is assigned to more than one User Profile, the user will have the option to select the profile during the login process. If the user is only registered with one User Profile, the user will be automatically logged into the corresponding User Profile.

In the image below, the user how to input a username and password that is associated with multiple User Profiles. In this example, the user is a member of both the “Default User Profile” and “Supervisors.”

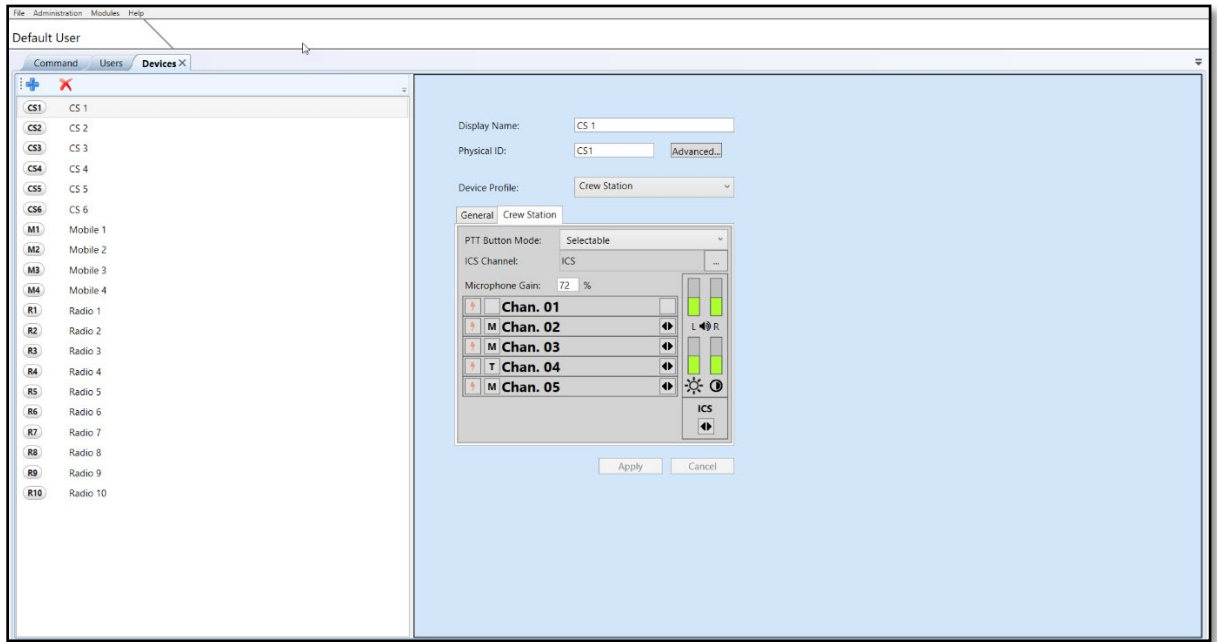


Upon selecting the desired profile, the user will now have access to the corresponding permissions and resources as created within the User Profile Editor.

### 5.3 Device Editor

The RADIUS Device Editor allows the system administrator to configure radio devices, crew stations, and mobile crew stations using the RADIUS crewstation app. To open the Device Editor, select Device Editor from the Administration menu.

The Device Editor is shown below:



On the left-hand side, the existing devices are displayed. The right-hand side area consists of the selected device configurations. In the image above, Crewstation #1 is selected. Device configurations such as Channel Assignment, PTT Button Mode, Microphone Gain, and other configurations are displayed.

All devices have the following configuration settings:

- **Display Name:** The name that appears within the graphical user interface.
- **Physical ID:** The name of the system to sort the assets within the graphical user interface. Within the Assets Module, the devices are sorted alphabetically based on the Physical ID of the device grouping: Crewstations, then Mobile Crewstations, then radios.
- **Advanced:** Includes user IDs and passwords for devices requiring these configurations.
- **Device Profile:** The type of device to be configured.

The following sections outline how to configure devices within RADIUS.

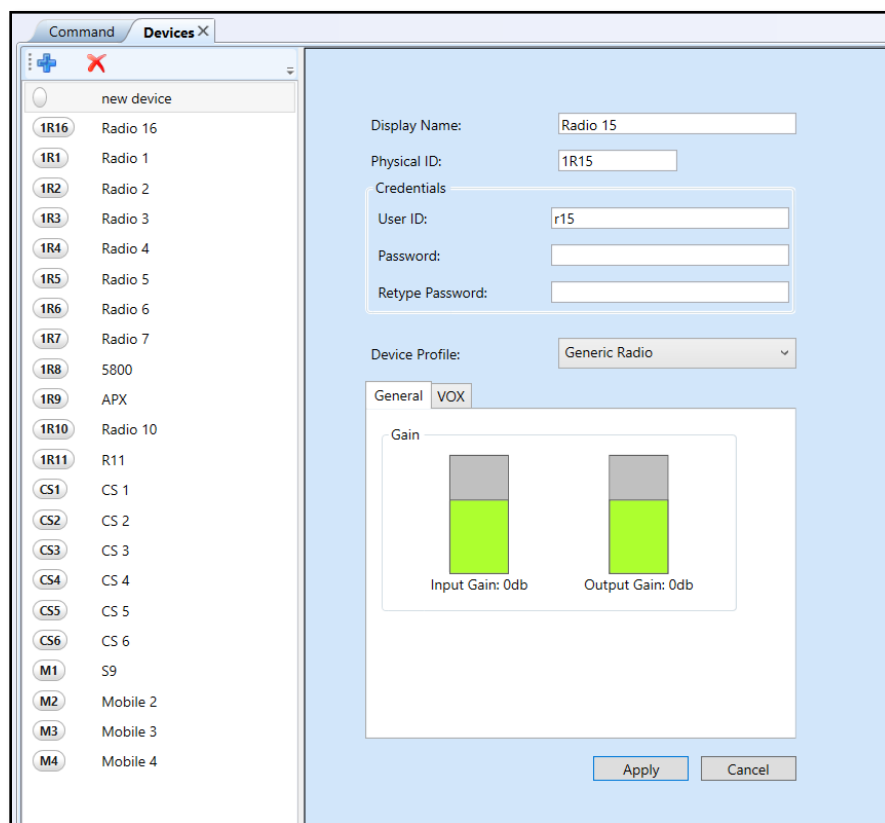
### 5.3.1 Radio Device Configuration

Radio Device Configuration refers to the configuration interfaces of a radio physically connected to the RADIUS DS. Radio Device Configurations will result in how the DS interacts with the tethered radio device. Configurations such as VOX, gain, and radio timings are found within the “General” tab of the Radio Device Configurations.

To configure a radio device:

1. Select an existing radio device or create a new device by selecting the “+” located within the Device Editor Tool Bar. For “Device Profile,” select “Generic Radio” from the dropdown menu.

The device configuration for the radio will appear as shown below.

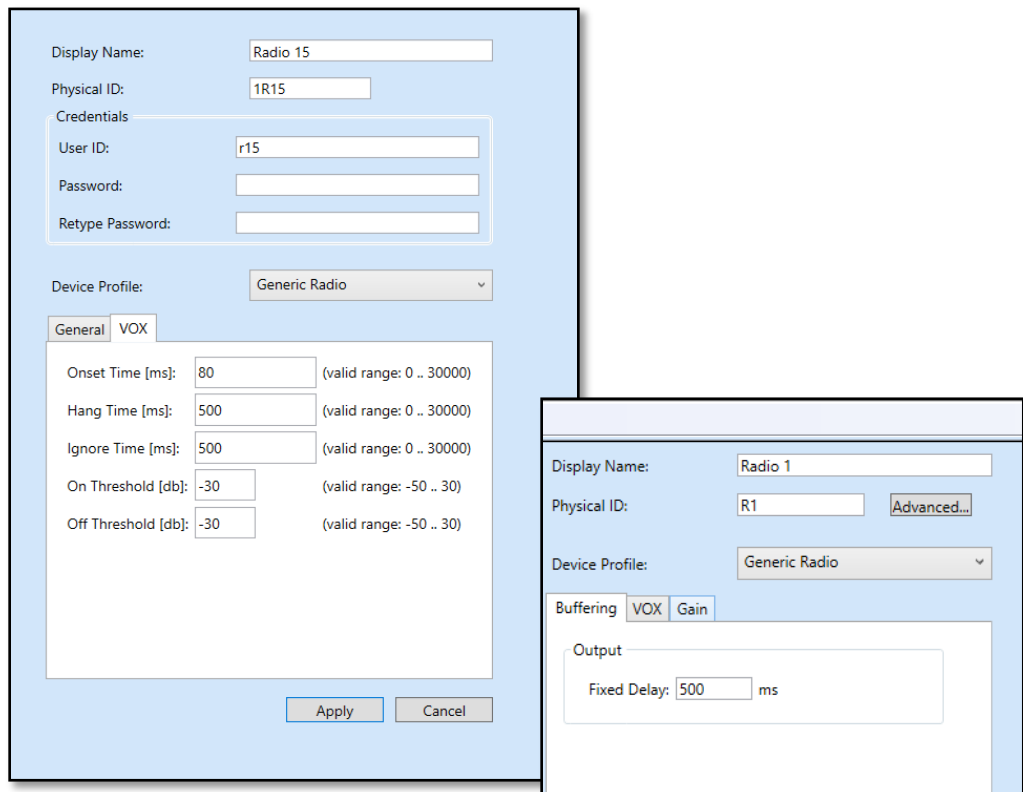


2. **Display Name:** Use the “Display Name” to rename the radio within the graphical user interface.
3. **Physical ID:** The Physical ID may stay the same or be edited to determine screen arrangement within the Assets Module. The Physical ID will be used to alphabetize the devices within the Assets screen.
4. **Priority:** Priority allows the system administrator to assign audio priority to a device. Within the dropdown, the administrator can set the highest priority, “1 – Highest Priority” so that incoming audio will be heard over lower-priority devices.

The priority list works in this manner whereby the preceding priority device has priority over the latter. When the device is added to a channel, the priority will be applied to the device within the channel.

To set a priority for a device, select the desired priority and select “Apply.” The system will restart the radio interface board (RIB) to apply the change.

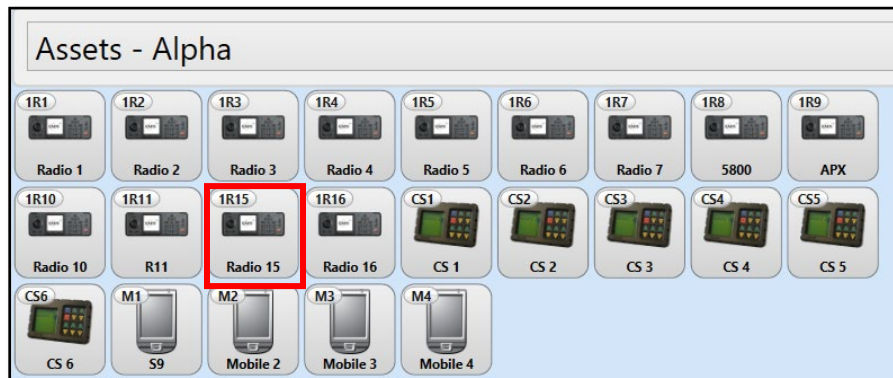
5. **Credentials:** For the radios to be available within the Command interface and have port visibility from within the LCD or Status Indicator, the asset must be verified with credentials. **Within the Credentials field, the User ID is set to “rx” by default where “X” is the radio port number. The default password is the same “rx” identifier.** For example, in the image above, the User ID is “r15” and the Password is input as “r15” with a “Retype Password” of also “r15.” Note that after the password is applied it will be shown as blank within the password fields.
6. **Device Profile:** Device Type allows the system builder or administrator to designate the type of device to be configured.
7. **Gain:** Within the “Gain” tab, the user may modify Input and Output gain by selecting the graphic. These settings are important as they will determine the audio quality and performance of the connected radio. By default, these values are set to 0dB and range from -50 dB to 30 dB.
8. **VOX:** Select the “VOX” tab to view VOX configurations. VOX configurations include Onset Time, Hang Time, Ignore Time, On Threshold, and Off Threshold.



**Buffering:** Within the Buffering tab, the administrator can place an outbound buffer on audio to compensate for delays related to the transmission of audio. This feature is recommended for trunking systems and PTT-over-cellular apps that require call set-up time.

9. Select "Apply." The setting for the radio device will be saved.

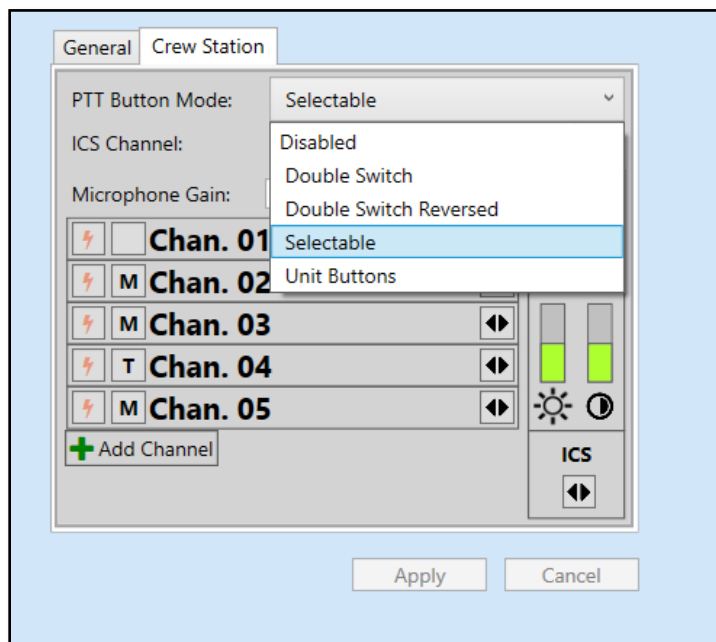
From within the Assets screen, the newly created device will be shown and sorted based on the Physical ID of the device.



### 5.3.2 Crew Station Device Configuration

The Crew Station Device Configuration allows the administrator to populate the necessary channels to the crew station.

The crew station configurations are shown below:



To configure the crew station:

1. Select the crewstation to be configured.
2. The default setting may remain. If it is a new crewstation, the User ID should be set to "cs0X" where X is the number of the crewstation port. The "cs" must be included.
3. Set the PTT Button Mode. Selectable is recommended for single-button PTT and handsets such as the H250 handset.
4. Input the desired channels by selecting the "+ Add Channel" button.

On the crew station, the populated channels will now be accessible.

If using the "Selectable," use the I and R buttons on the crewstation to determine the transmit patch. The selected path will be highlighted in red.

Use the "Microphone Gain" setting to control the level of the input audio from the connected CS microphone.

### 5.3.3 Mobile Crew Station Device Configuration

The mobile crew station configurations are shown below:

Similar to the tethered crewstation, the Mobile Crewstation allows for channels to be populated within the device-specific assignment. It is important to note that within the Mobile Crewstation the following parameters must be set:

Advanced: User ID and password must be configured to match the application.

PTT Button Mode: Must be set to “Double Switch” for proper operation of the “ICS” and “Radio” buttons on the application.

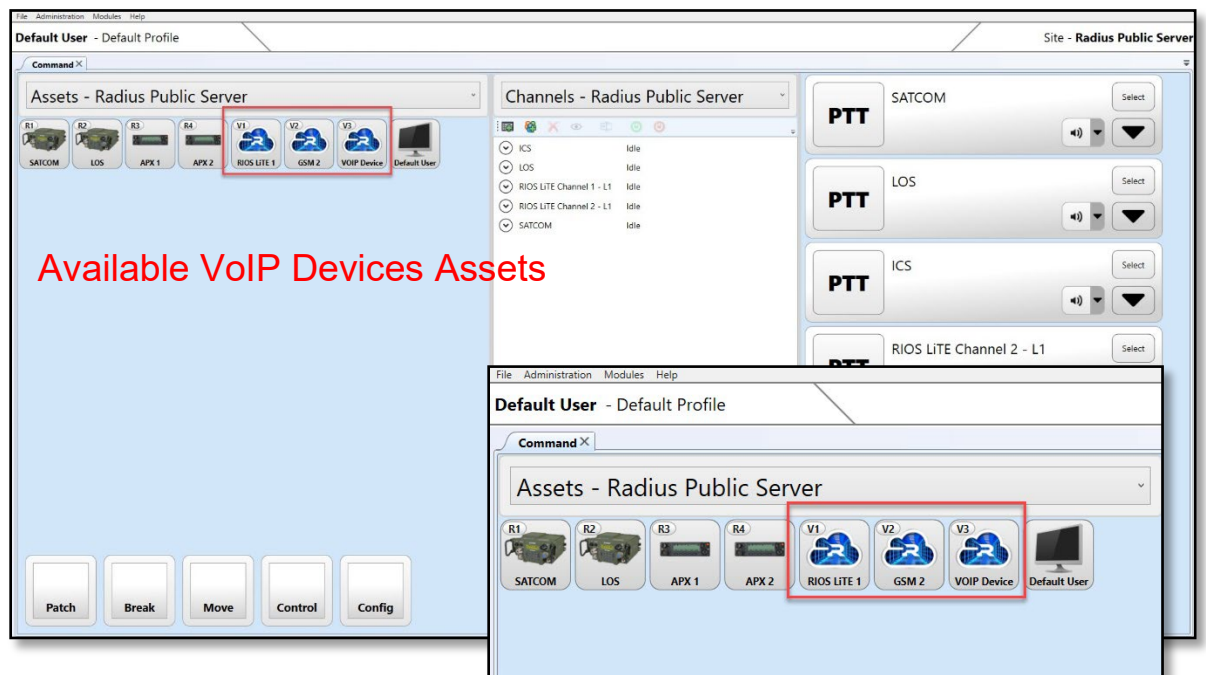
The screenshot shows a configuration window for a Mobile Crew Station. At the top, there are input fields for 'Display Name' (S9) and 'Physical ID' (M1). Below these is a 'Credentials' section with fields for 'User ID' (S9), 'Password', and 'Retype Password'. A 'Device Profile' dropdown menu is set to 'Mobile Crew Station'. The main configuration area is divided into two tabs: 'General' and 'Crew Station'. The 'Crew Station' tab is active, showing 'PTT Button Mode' set to 'Double Switch', 'ICS Channel' set to 'ICS', and 'Microphone Gain' at 0%. Below these are seven radio channels, each with a status icon (M or T) and a name: Radio 1 (M), Radio 2, Radio 3, Radio 4 (T), Radio 5 (M), Radio 6, and Radio 7 (M). To the right of the radio list are volume sliders for 'L' and 'R', a brightness icon, and an 'ICS' button. At the bottom of the dialog are 'Apply' and 'Cancel' buttons.

### 5.3.4 VoIP Devices

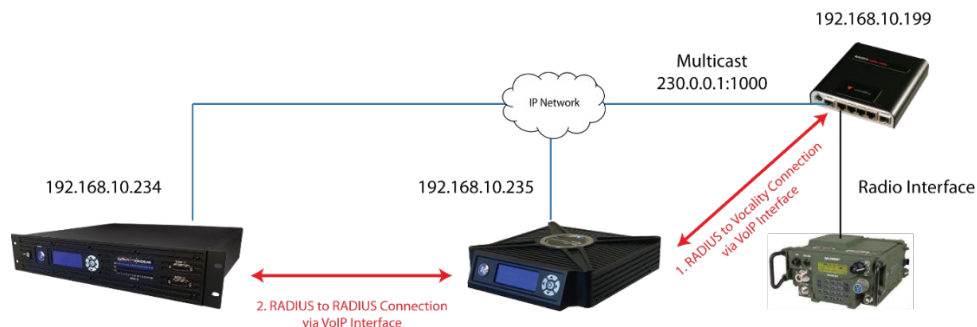
VoIP Devices in RADIUS refer to an external device communicating with the RADIUS gateway over IP. RADIUS utilizes a virtual device to represent the licensed connection to the IP device. IP devices can include a Vocality ROIP device, ETC microphone, or RIOS Server. The number of licensed VoIP Devices appears within the License Key found within Administration > Change Server Settings > Licensing.

When a virtual device is added through the Device Editor, the RADIUS gateway will internally create an instance of the device. The device will then connect and communicate with the server's API. The virtual device can then function as a radio asset whereby the operator can patch or place the virtual device radio into a channel for standard operation.

In the example below, four VoIP Devices are created and connected to various VoIP connections.



In the example below, RADIUS is communicating with a Vocality radio gateway and another RADIUS Gateway over an IP connection as well as another RADIUS gateway.





In this example, two VoIP connections are occurring:

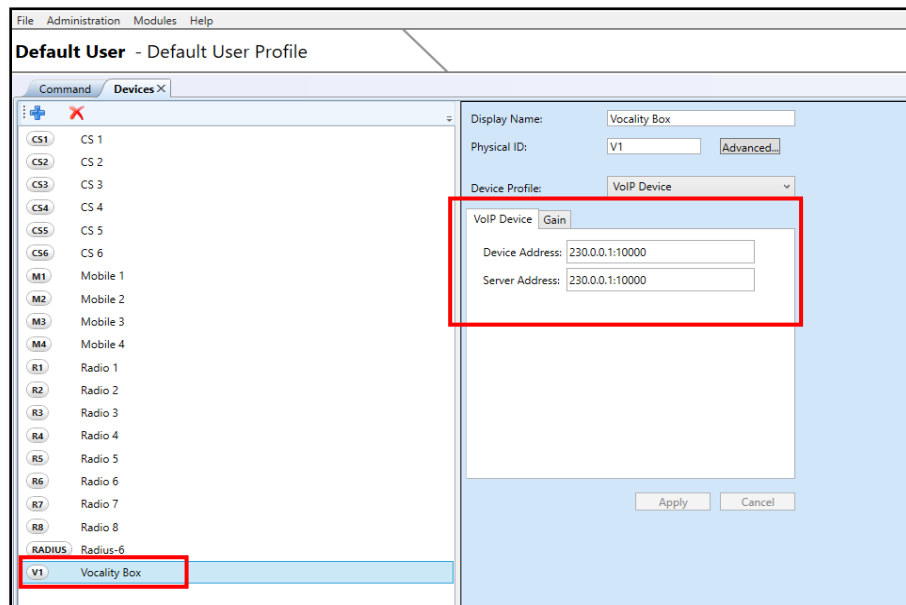
1. A Vocality to RADIUS Gateway Connection: This connection allows RADIUS to access the radio interface physically connected to the Vocality gateway. A multicast address is enabled to allow RADIUS to utilize a VoIP Device for interoperating with the Vocality network.
2. A RADIUS-to-RADIUS connection is made by configuring a virtual VoIP Device on each system.

To Configure a Vocality Connection:

1. From the Administration menu, select **Device Editor**.
2. If a VoIP device is not already created, select the “+” sign.
3. Input the Display Name, and Physical ID (where it will appear alphabetically within the Assets module), and provide a user name and password for the device, for example, “v1” and “v1” for the example below.
4. In the VoIP Device tab, **input the VoIP Device receive IP address and port**. In this case, it’s the multicast address and port of 230.0.0.1:10000. An example of unicast would be 10.0.0.20:10000.

**Input the RADIUS Server to receive the IP address and port.** In this case, it’s 230.0.0.1:10000. An example of unicast would be 10.0.0.10:10000.

Verify that the IP and port number are separated by a colon and no spaces. This appears as:



- 
5. Select **Apply.** The VoIP Device will be visible as a Radio Asset from within the Command Screen. To test, transit from a field radio to the radio connected to the Vocality gateway. If the asset turns green, the connection is operational.

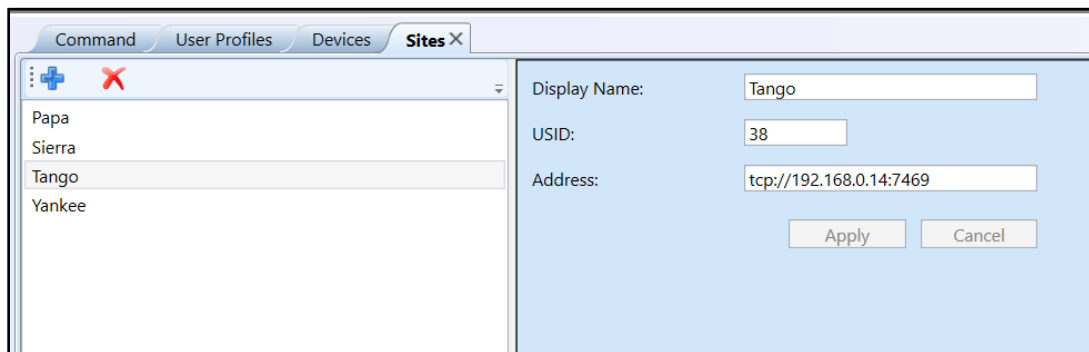
The operator is then able to patch or place the VoIP Device into a channel.

## 5.4 MultiSite and Site Editor

RADIUS Multisite enables the RADIUS gateway to be federated across an IP network. With this configuration, operators logged into a local RADIUS gateway can, if permissioned, monitor, patch, and control assets connected to a remote RADIUS gateway.

The Site Editor Allows the administrator to add, delete, or modify the IP connections to RADIUS Gateways connected in a RADIUS MultiSite.

In the image below, the Site Editor contains four sites. If the operator selects a site, the site information is shown to the right.



**Display Name:** The name of the remote site and how it is shown on the local client

**USID:** The unique system ID of the system. This can be accessed from the front LCD panel on the gateway.

**Address:** The IP address of the remote site. The system will connect to port 7469. If a firewall is utilized, port forwarding for port 7469 might be required.

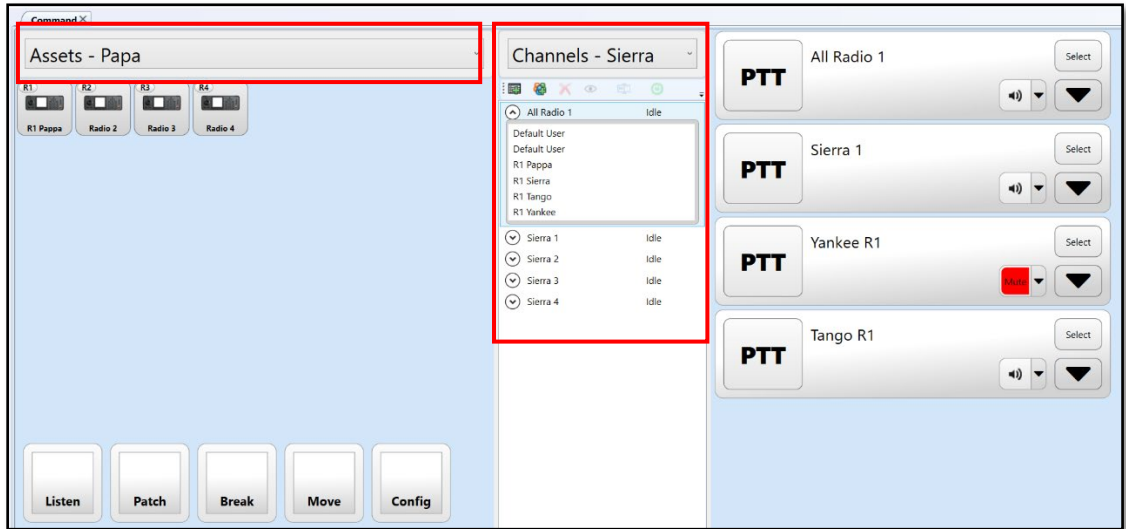
The image below displays the RADIUS GUI with access to the above RADIUS MultiSite configuration. From the dropdown, the operator can choose the site to view or access the remote site's Assets. In the Channels Module, the dropdown allows the operator to view remote channels and select them for their Dashboard.

### To Add a Site:

1. Select the Site Editor from the Administration tab.
2. Select the "+" sign to create the new site.
3. Select "new site" from the site list.
4. Input the Display Name of the new site, the USID of the new site, and the IP address as tcp://\_\_\_\_\_:7469.
5. Select "Apply."

- Repeat the process from the other gateway.

If added correctly, the Assets and Channels will appear in each site's drop-down.

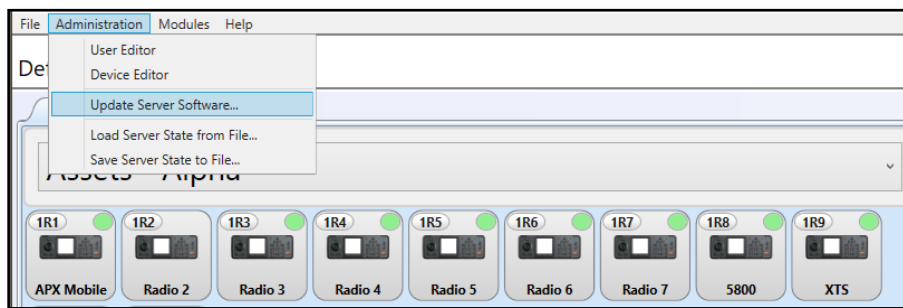


## 5.5 Updating the RADIUS DS and Crewstation

RADIUS allows the system administrator to update the DS software from within the RADIUS Client.

To update the DS Software:

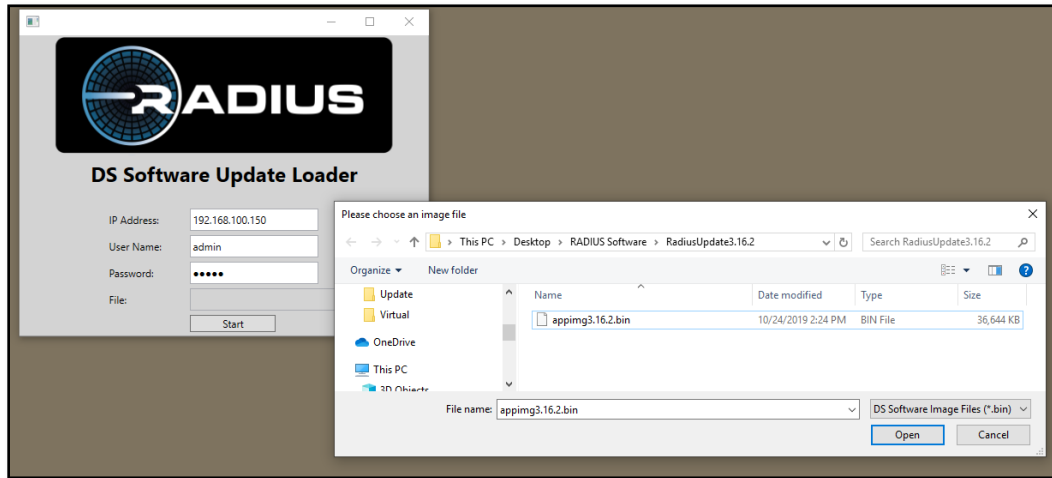
- Select the "Update Server Software" from the Administration tab.



The DS Software Update Loader may also be located in the "Radius" folder found within Program Files. Run the "Radius.Client.UpdateLoader" application to access the DS Updater.

- The "DS Software Update Loader" will be displayed as shown below. Input the IP address of the DS and the User Name and Password of the account with DS Update rights.

3. Select the “...” to load the desired “appimg.bin” file that contains the DS image. In the example below, the RADIUS version is 3.16.2. Select “Open.”



4. Select “Start.” The DS Updater will begin the update process.
5. When complete, the DS Updater will instruct the admin to restart the DS. The DS will supply the image to the Crewstation. The process may appear to restart the crewstation.

Note: If the DS Update responds with “ApiPduSynchronizer server request has timed out,” the network switch may not be able to pass the required data. Disconnect from the switch connect directly to the Ethernet port of the DS and run the update.

6. If a RADIUS Client update is available, update the client with the corresponding .msi file.

## 5.6 Changing the External DS IP Address

The RADIUS DS IP address may be changed to communicate with the desired network. The DS must be assigned an IP address that will not conflict with other devices on the network. By factory default, the RADIUS DS is set to 192.168.1.10.

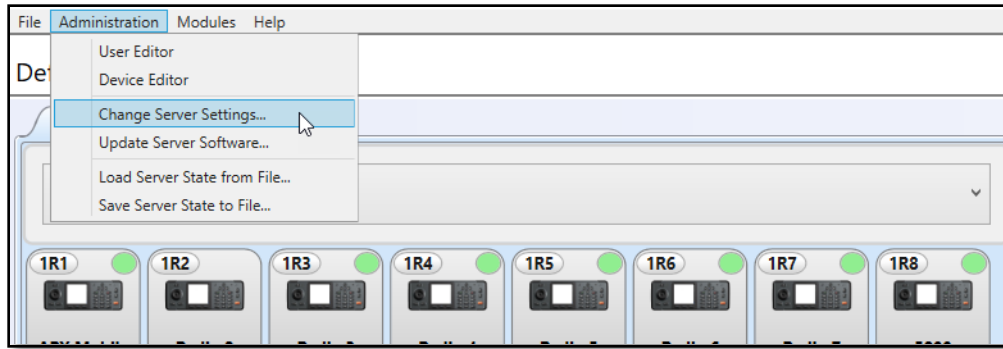
The internal IP address scheme of the DS, radio interface boards (RIBs), and crew stations reside in the 192.168.100.X range. Because of this arrangement, the external IP address cannot be within the 192.168.100.X range of addresses.

To change the external IP address of the DS:

1. Log on to the DS with the RADIUS client application.

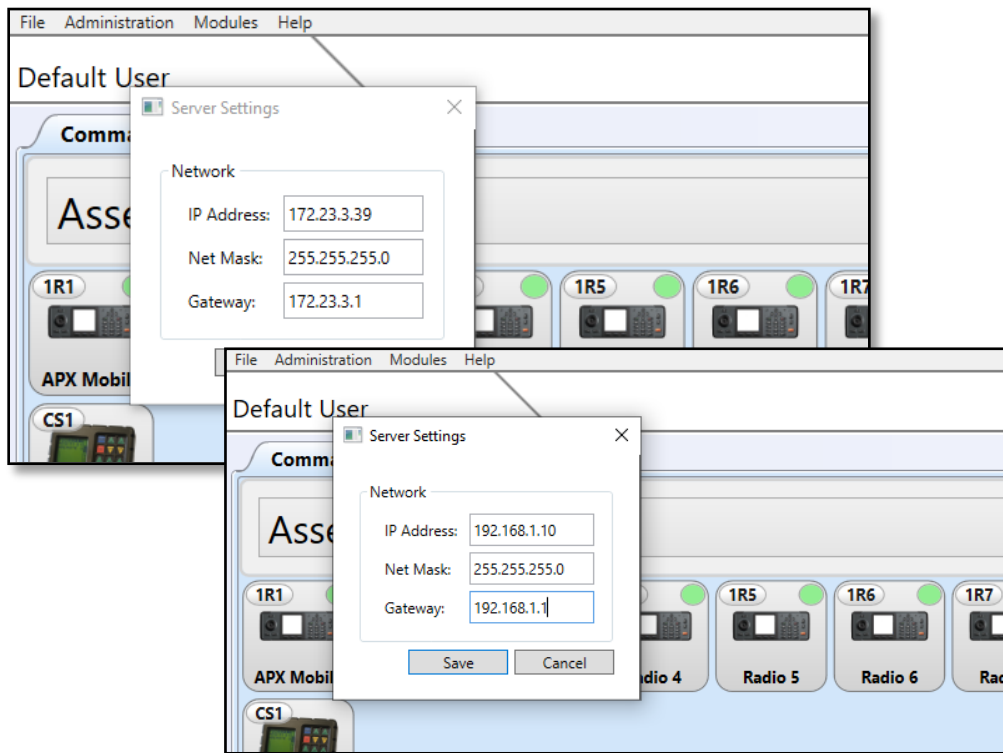
The computer operating the client application must be able to access the IP of the DS and the client application must be configured to access the DS IP address. See Step 4 below for how to change the client's IP

2. From the Menu Bar, select “Administration,” and “Change Server Settings.”



3. Input the desired IP address, subnet mask, and gateway.

In the example below, the admin is changing the External DS IP address from 172.23.3.39 to 192.168.1.10. Currently, the computer operating the RADIUS client is configured for a 172.23.3.X address. After the DS IP is changed, the client will no longer be able to access the DS. The RADIUS client will need to be reconfigured to point to the new DS IP. For more on this topic, please see the section below titled, “Changing the Client DS IP Address.”



4. After the correct information is input, select “Save.”
5. Restart the DS. The IP address will now be set to the new address.

### 5.7 Restarting the DS

The operator can restart the DS remotely from within the RADIUS Client. Select Administration, Change Server Settings, and within the Network tab, select “Restart Service.”

## 6. MODIFYING THE RADIUS CFG FILE

The RADIUS cfg file allows the administrator to set various pre-configurations for the RADIUS Client. These settings include but are not limited to, setting the auto login, auto username and password, port addresses, and determining a PTT trigger such as a foot pedal.

### 6.1 Accessing the RADIUS Client cfg File

1. Close the RADIUS Client application if open.
2. Locate the “RadiusApp” folder located at:

Local Disc (C) > Users > RADIUS > AppData > Roaming> SyTech > RadiusApp

Tip: Type “%appdata%” after clicking the Windows Start button to access the “SyTech” folder.

3. Right-click on the file titled: “radiusAppConfig.json.”
4. Select “Open with.” Select a text editor program such as Notepad. The RADIUS application configuration data will be shown.

### 6.2 Set Auto Logon Setting

Auto Logon settings allow the operator to bypass the initial log-on screen or input credentials. Below is an example of a log-on that will auto-fill the username and password.

```
"AutoLogonEnabled": false,  
"AutoLogonUserId": "admin",  
"AutoLogonPassword": "admin",  
"AutoLogonHost": "192.168.1.10",
```

### 6.3 Set a PTT Trigger Device

If a PTT trigger device such as a foot pedal or PTT button is utilized, the following cfg field can be modified as shown.

```
"FootPedalPttTrigger": {  
  "SerialPort": "COM4"
```

Where COM4 is the device port found within the Windows Device Manager.

### 6.4 Virtual Control Head Layering

The user may elect to change the layering for the Virtual Control Heads. The user can select if the VCHs operate as standard windows within the interface (“false”) or appear

above all other windows outside of RADIUS (“true”). The “True” setting also enables the VCHs to be accessible when the client is minimized.

*"ShowControlHeadsTopMost": false,*

When complete, save the modified radiusAppConfig file and start the RADIUS Client.

## 6.5 Enabling TLS on the Radius Client

RADIUS can be configured for TLS depending on the factory’s system configuration. Encryption **on the DS** can not be changed by the administrator. Contact SyTech if system encryption is necessary.

By default, the client configuration is not set for TLS. If the DS is configured for TLS, the “RadiusAppConfig” text file will need to be enabled for TLS.

The text below provides an example of the default Radius cfg for Radius Client. To enable TLS, indicate “true” in the line as shown. Save the file and restart the client.

```
{
  "AutoLogonEnabled": false,
  "AutoLogonUserId": "admin",
  "AutoLogonPassword": "admin",
  "AutoLogonHost": "",
  "TlsEnabled": true,
  "SsiPort": 5151,
  "ApplicationName": "Radius Client",
  "UplinkController": {
    "BinTcplfClient": {
      "ServerIp": "192.168.100.150",
      "ServerPort": 7467,
      "ReconnectTimeMs": 3000
    },
    "RadiusSession": {
      "ClientId": "N/S",
      "PreferredMediaAddress": "rtptcp://127.0.0.1:30000",
      "UseMulticast": false,
      "UserAgentName": "unspecified",
      "SessionTimeoutS": 10
    }
  },
  "FootPedalPttTrigger": {
    "SerialPort": ""
  }
}
```



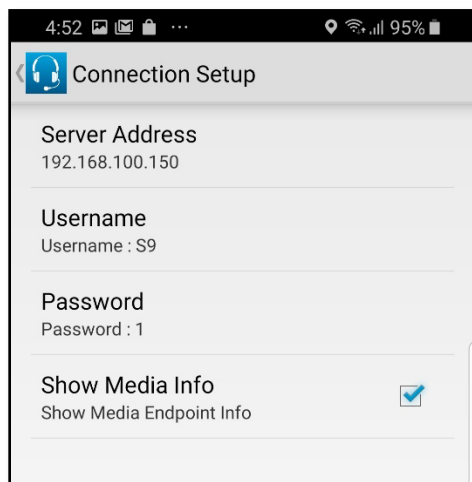
## 7. RADIUS MOBILE CREWSTATION APPLICATION

The RADIUS Mobile Crewstation Application enables wireless crewstation-like functionality from an Android smartphone. The Mobile CS App operates via WiFi and UDP/TCP connection from the smartphone device to the RADIUS DS.

### 7.1 Connecting the Mobile Device

To connect the RADIUS Mobile Crewstation Application:

1. Install the SyTech RADIUS Mobile Crewstation App. The application may be placed in the Downloads or other folder on the smartphone.
2. Start the RADIUS Mobile CS App. The login screen will appear and indicate “Offline.”
3. Select the menu button located at the top right of the login screen.
4. Select “Settings.”
5. Select “Connection Setup.” An example configuration is shown below.



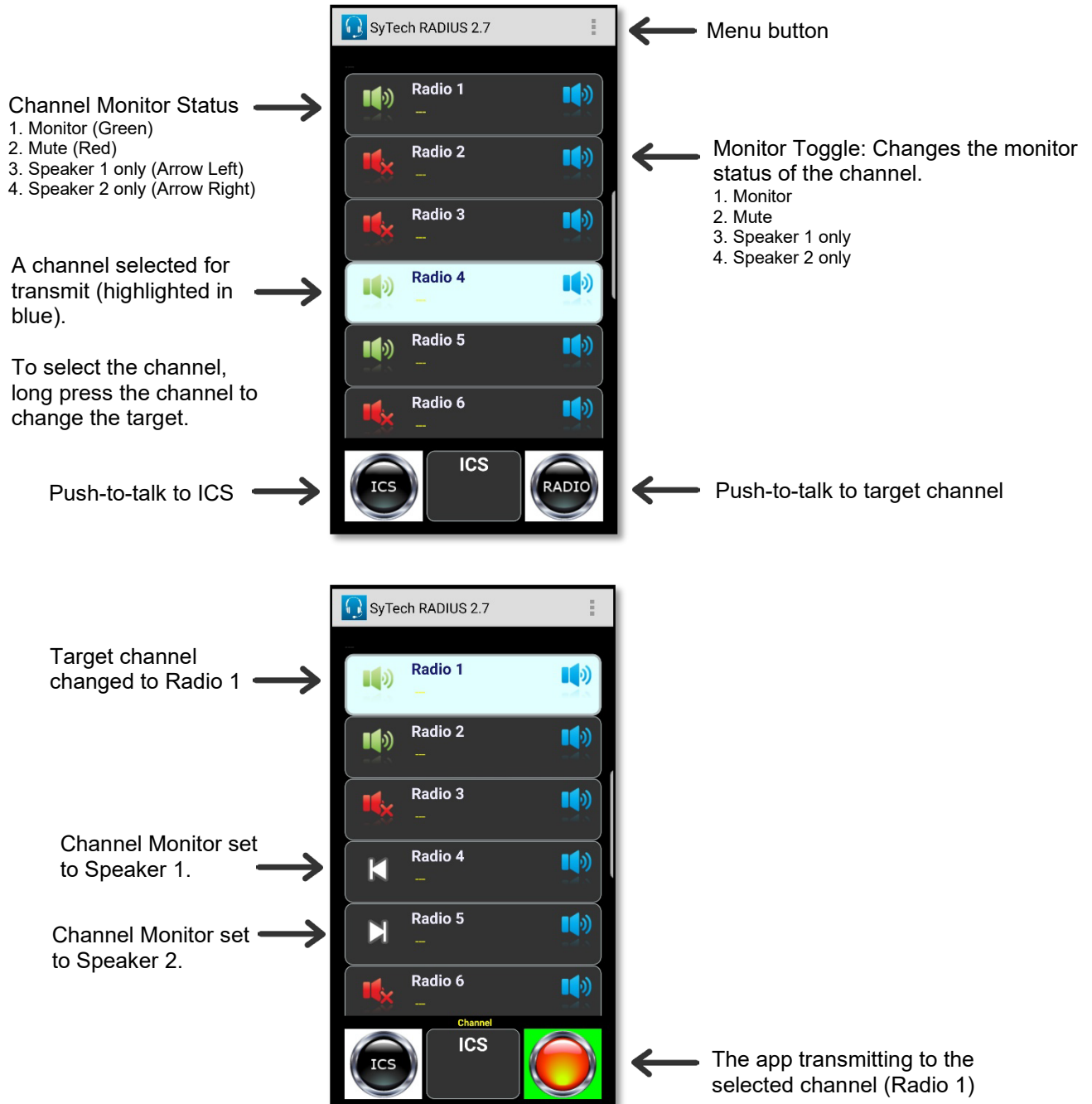
6. By default, the RADIUS DS Server Address is 192.168.100.150. The Username and Password must match the User ID and Password found with the “Advanced” settings of the corresponding Device Profile within the Device Editor (see the section titled “Mobile Crew Station Device Configuration” for how to configure the device profile)
7. Select the back button to return to the login screen.
8. Select the menu button, “Log On.”

If configured correctly, the channels that were populated within the Device Editor will be shown. If no channels are shown, confirm within the “Crewstation” tab of the corresponding Mobile device found within the Device Configuration.

## 7.2 Using the Mobile App

The RADIUS Mobile Crewstation Application replicates the functionality of the physical RADIUS Crewstation. For example, the channels shown within the app are populated by the DS. A channel can be selected as the target channel (long press, the channel is highlighted), and a set-aside ICS channel may be designated.

The image below illustrates the RADIUS Mobile CS App.



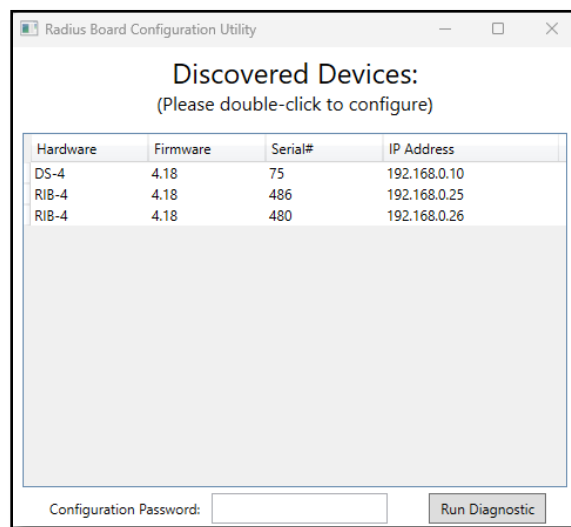
Note: By design, the user can not toggle the monitor state of the selected channel. To toggle the selected channel, the user must select another channel (long press) and then toggle the desired channel state.

## 8. RADIUS BOARD CONFIGURATION UTILITY

The RADIUS Board Configuration Utility refers to a standalone application that allows advanced system administrators to configure the IP settings of Radius devices including nPoints, Radius DSs, and Radius Crewstations.

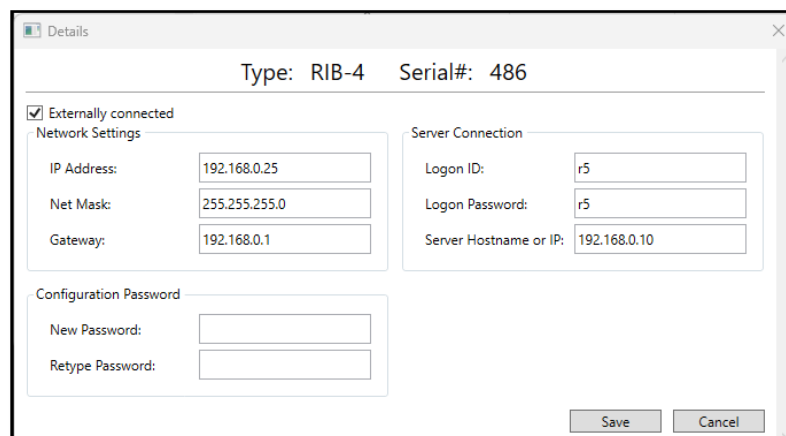
Upon installing the Radius Client, the Radius Board Configuration Utility can be found in the C:/Program Files (x86)/SyTech folder. Double-click the application titled, "Radius.Tools.BoardConfig.BoardConfigUtil."

The utility will search the network for available Radius devices. In the graphic below, the utility has located three devices, one DS (Distribution Server) and two RIBs (Radio Interface Boards). The firmware, serial number, and IP address of the devices are indicated.



### 8.1 Change the IP Address of a Device

1. Double-click the device to modify.
2. Check "Externally Connected" to access the device details. The device details will be shown as below.



3. Input the desired IP address into the Network Setting, changing the necessary configurations as needed.

The “Network Settings” refer to the setting of the device. This includes the IP address of the device, subnet mask, and outbound gateway.

4. The “Server Connection” refers to how the device will log on to the corresponding DS. The “Logon ID” and “Logon Password” refer to the settings found within the Device Editor within the Radius Client. If a new device is being added (see the section below for more information on how to add the device in the Radius DS) add the device information in the ID and password fields. By convention, the fifth RIB is called “r5” with password “r5” and the sixth RIB is “r6” / “r6” etc.

The “Server Hostname or IP” is the address of the Radius DS. This information must be correct for the RIB to correctly appear within the DS.

5. Select “Save.” The device will reset (if it does not reset, manually reset the device).

## **8.2 Add a New Device to the Radius DS**

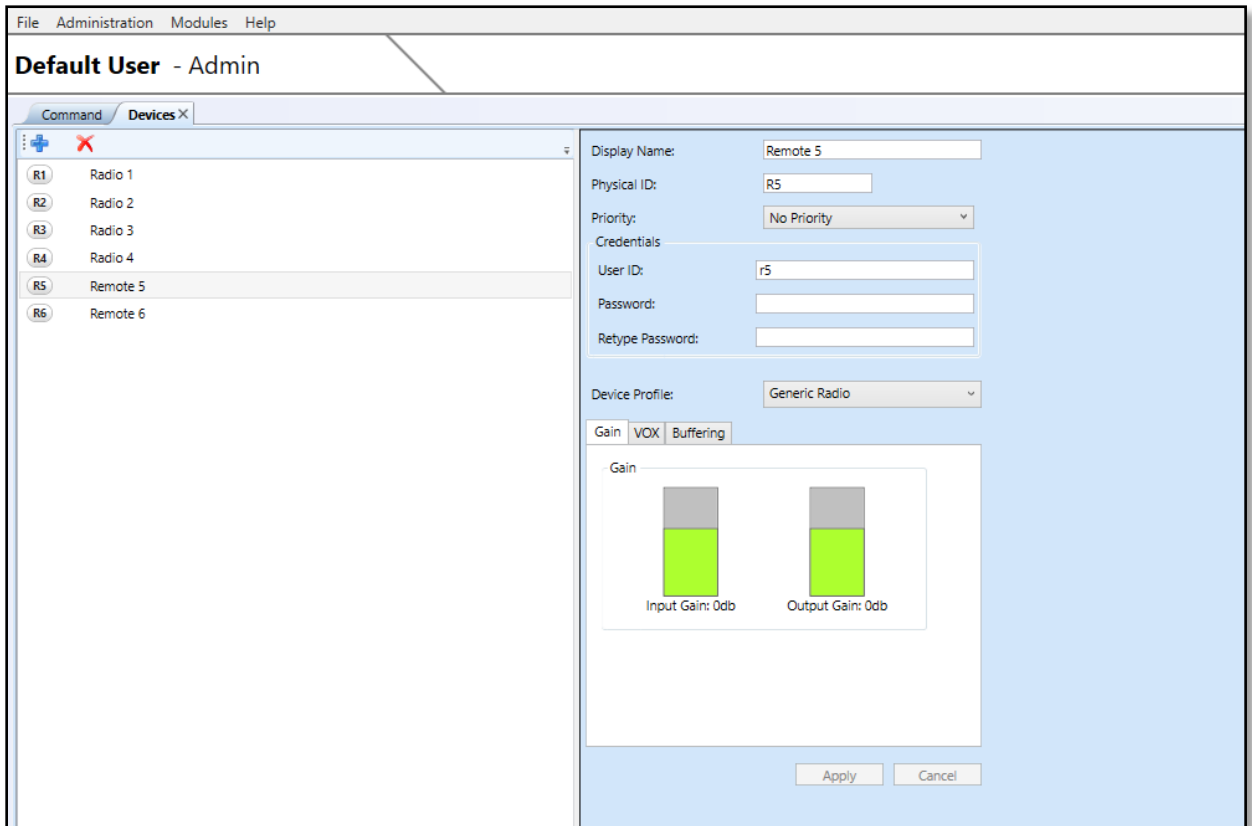
Add the newly configured device to the Radius DS via the Radius Client.

In the example above, the Logon ID and Password are “r5.” This corresponds to the settings found within the Device Editor.

To Add the New Device to the Radius DS.

1. Log into the Radius Client.
2. From the Administration tab, select Device Editor.
3. Select the “+” to create the new device.
4. Select the “new device.”
5. For additional assistance, follow the steps found within Section 5.3.1 “Radio Device Configuration.” Within the “Credentials” portion of the configuration, use the User ID and Password as configured in the previous step. For example, “r5” and “r5” for both fields.

The image below a new RIB titled “Remote 5” is being created in the Device Editor.



6. When complete, select “Save.”

If the new device is connected and configured correctly it will appear in the Command tab with the other Assets. The blue DS service light will appear on the nPoint or 2U front panel if the device is added correctly.

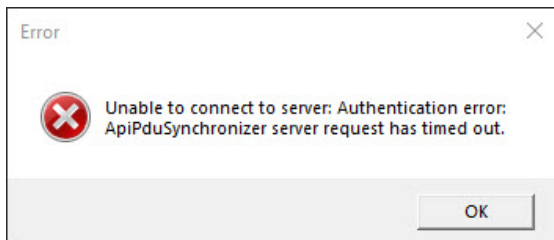
Restarting the server after adding a new device is not necessary. If the RIB does not appear, restart the devices, and confirm all blue DS service lights are lit and the configuration is correct.

## 9. COMMON SUPPORT ISSUES AND TROUBLESHOOTING

The following symptoms refer to possible issues with operating RADIUS.

### LOGGING IN

**Symptom:** When attempting to log in to the client, the system responds with “Unable to connect to Server: Authentication error: ApiPDU synchronizer server request timed out.”



**Reason:** The Client cannot locate the server.

**Resolution.** Confirm that the client computer can ping the IP address of the server using a Command Line Prompt. If the server can not be reached verify that the network settings are compatible with the gateway (you may need to change the IP of your computer temporarily to match the IP settings on the gateway). See Section 5.5 for instructions on how to change the External DS IP Address.

### AUDIO

**Symptom:** Only color indicators such as green and red for asset receive. No audio but the data is flowing.

**Reason:** Prior to RADIUS Client 4.12 the default transport was UDP. If the client is an older version or UDP transport is preferred, the network may not allow for UDP transport or the 50,000 ports are not open. The data is passed via TCP and that's why we see the color changes but no audio.

**Resolution:** Change the client to TCP.

1. Close the RADIUS Client app if open.
2. Go to the AppData folder on your PC. One way to do this is to type "%appdata%" in the Windows search.
3. Within the folders, go to SyTech > RadiusApp.
4. Open the file titled "radiusAppConfig."
5. Change the PreferredMediaAddress to read:

```
"PreferredMediaAddress": "rtptcp://127.0.0.1:30000",
```

6. Save the file.

---

7. Restart the RADIUS Client app.

Try the radios again.

**Symptom:** When keying a channel or asset, the channel or asset does not turn red to transmit until the operator releases the PTT.

**Resolution:** The client does not detect a microphone connected to the computer operating the client. Close the client and connect a microphone, restart the client, and test.