RADIUS Client Manual

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

March, 2026

For RADIUS Software Version 5

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

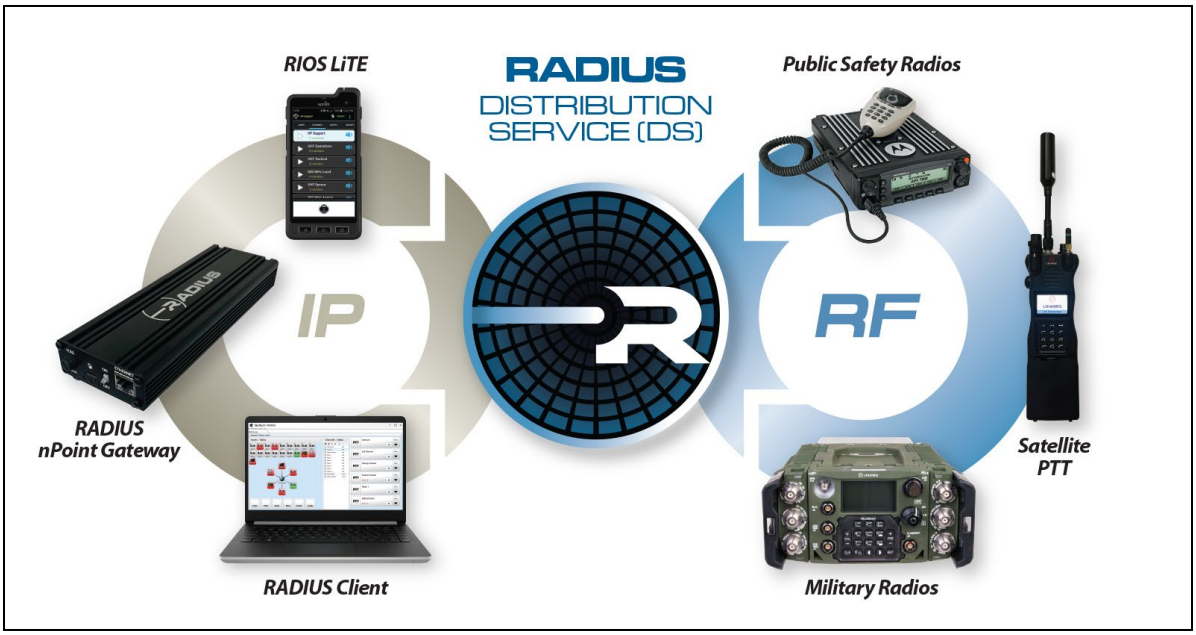
All rights reserved.

TABLE OF CONTENTS

1. RADIUS OVERVIEW

The SyTech Radio and Digital Intercom Unified System (RADIUS) is a communications platform that interconnects radios, computers, smartphones, and crewstation intercom systems. By linking these devices through a common network, RADIUS enables interoperable voice communications between otherwise incompatible systems.

RADIUS operates on a Linux-based hardware and software architecture. System configuration and operation are performed through a network connection using a personal computer running the RADIUS Client application.



The system allows users to communicate through multiple types of endpoints. These include analog devices such as two-way radios, as well as IP-based devices such as computers, smartphones, and the RADIUS crewstation intercom. Together, these components form a communications network that allows users on different device types to communicate with one another.

The illustration below shows a typical RADIUS system configuration connecting radios, smartphones, computers, and a RADIUS crewstation.

This document describes the operation and functionality of the RADIUS software. For information about specific hardware components included in your system, refer to the corresponding RADIUS Hardware Manual.

For additional assistance, contact SyTech at 703-941-7887.

2. CLIENT SOFTWARE INSTALLATION

The RADIUS Client application allows users to access and control the RADIUS system from a Windows-based personal computer. The following prerequisites are required to install and operate the RADIUS Client:

- Windows 11 – As of January 2026, all new RADIUS systems are configured for TLS 1.3 and require Windows 11 for secure client connections.

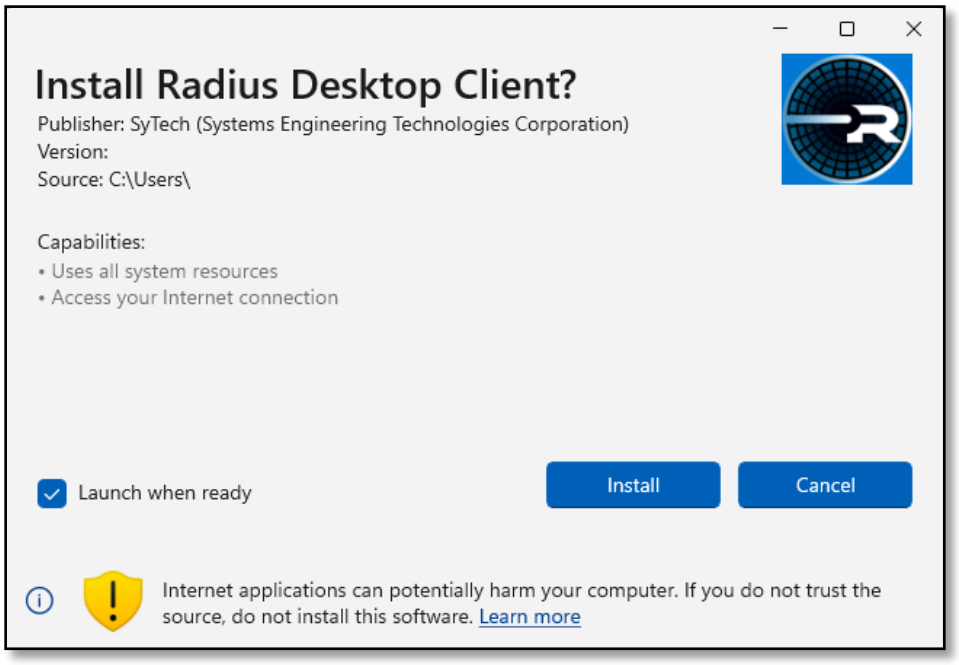
- Network connection – The personal computer must have IP connectivity to the RADIUS Distribution Service (DS) Gateway. The client system must be able to communicate with the DS gateway over the network.

Quick Tip: RADIUS Network Ports

TCP Ports (default): The RADIUS Client uses TCP ports **7467** and **7468** for audio receive and transmit. After the client successfully connects, the gateway assigns a dynamic port within the range of 49,153–65,555 for ongoing client communications.

2.1 Installing the RADIUS Client

1. Locate and double-click the "RADIUS Setup" (.MSIX) installation file. The software can be found on the SyTech website at: https://www.sytechcorp.com/RADIUSsoftware
2. The Windows installer will launch.

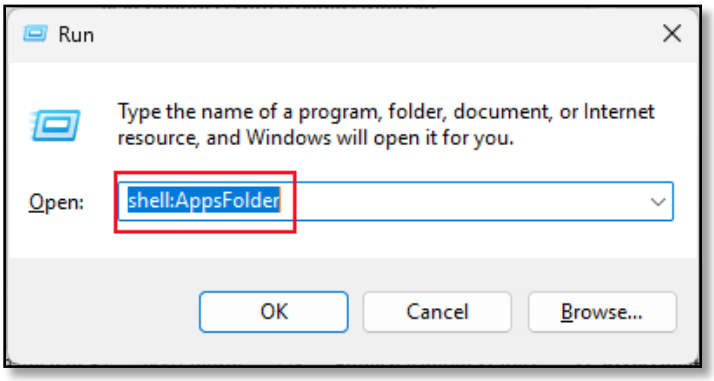


3. Follow the installation prompts and select the default options.
4. When the installation is complete, the application will automatically launch.

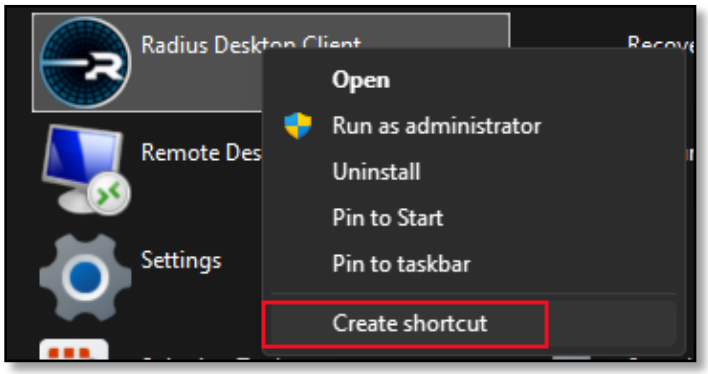
2.2 Creating a Windows Desktop Shortcut

An .msix package installs applications using the Windows App Installer system. Unlike older .exe or .msi installs, it usually does not let you directly place shortcuts during installation. Windows registers the app instead, and you create shortcuts afterward.

1. Press Win + R
2. Type:
   shell:AppsFolder



3. Press Enter. A folder will open showing all installed apps, including MSIX packages.
4. Right-click the RADIUS Client app.
5. Choose Create shortcut.



6. Windows will say it cannot create it in that folder and ask to place it on the Desktop.
7. Click Yes.

The shortcut will appear on the Windows Desktop.

3. RADIUS CLIENT SOFTWARE BASICS

This section provides an overview of accessing the RADIUS Client and introduces the basic elements of the graphical user interface (GUI).

3.1 Logging In

1. Launch the RADIUS Client by double-clicking the RADIUS icon on the Windows taskbar, or by searching for "RADIUS" in Windows Search.
2. The RADIUS Login window will appear.
3. By default, the User ID is admin and the password is admin.
4. In the Site field, enter the IP address of the RADIUS server. The gateway's LCD screen displays this value as "IP Address." Most systems are configured with the default address 192.168.0.10.

The RADIUS Distribution Service (DS) IP address is also displayed on the front-panel LCD of the gateway. If the RADIUS gateway does not include a front-panel LCD, the administrator may use the RADIUS Board Utility (see Section 7) to scan the network and identify available RADIUS DS systems.

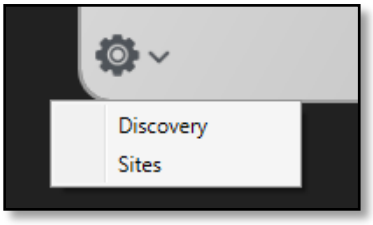
An example of a standard default login is shown below.

5. Select Logon.

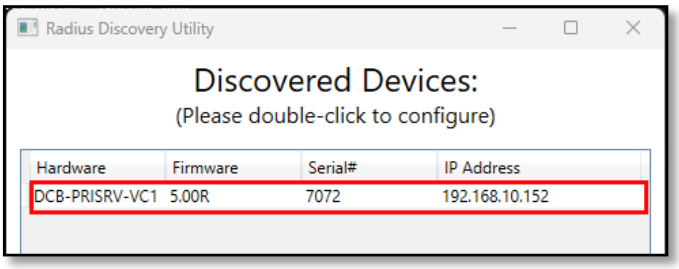
   If no additional User Profiles have been assigned, RADIUS will automatically log the user into their profile. If one or more alternative User Profiles have been assigned to the User, select the appropriate User Profile. See Section 5.2 for more information on User Profiles.

3.2 Login Options

In the lower-left corner of the screen, the Login Options icon (gear symbol) is displayed. This icon provides access to the Discovery Utility and the Sites list.

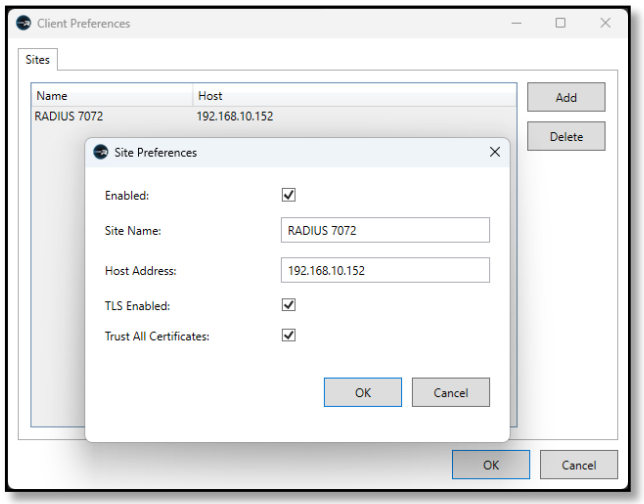


Discovery: Displays RADIUS sites available on the local network. If the system does not include an LCD screen and the DS IP address is unknown, use the Discovery Utility to locate available RADIUS Distribution Service (DS) systems.



Sites: Displays the list of sites saved on the client. Operators may add additional sites, which will appear in the Site drop-down menu after they are saved and initialized. By double-clicking a site entry, the operator can access additional configuration options, including assigning a site name, editing the IP address, and modifying security settings.

In the example below, the operator has double-clicked the site to open the Site Preferences. The recommended default settings are shown.



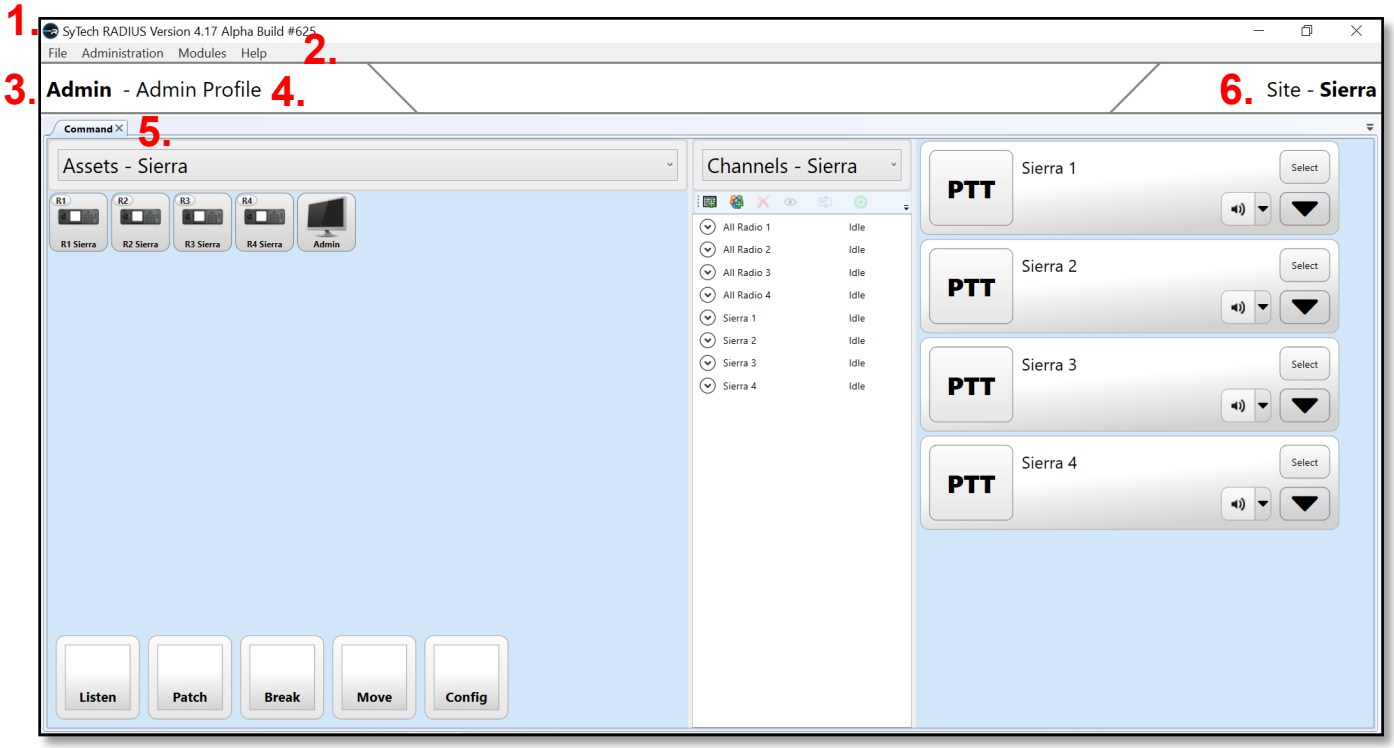
Additional login configuration options are available under File, Login Settings.

3.3 System Overview

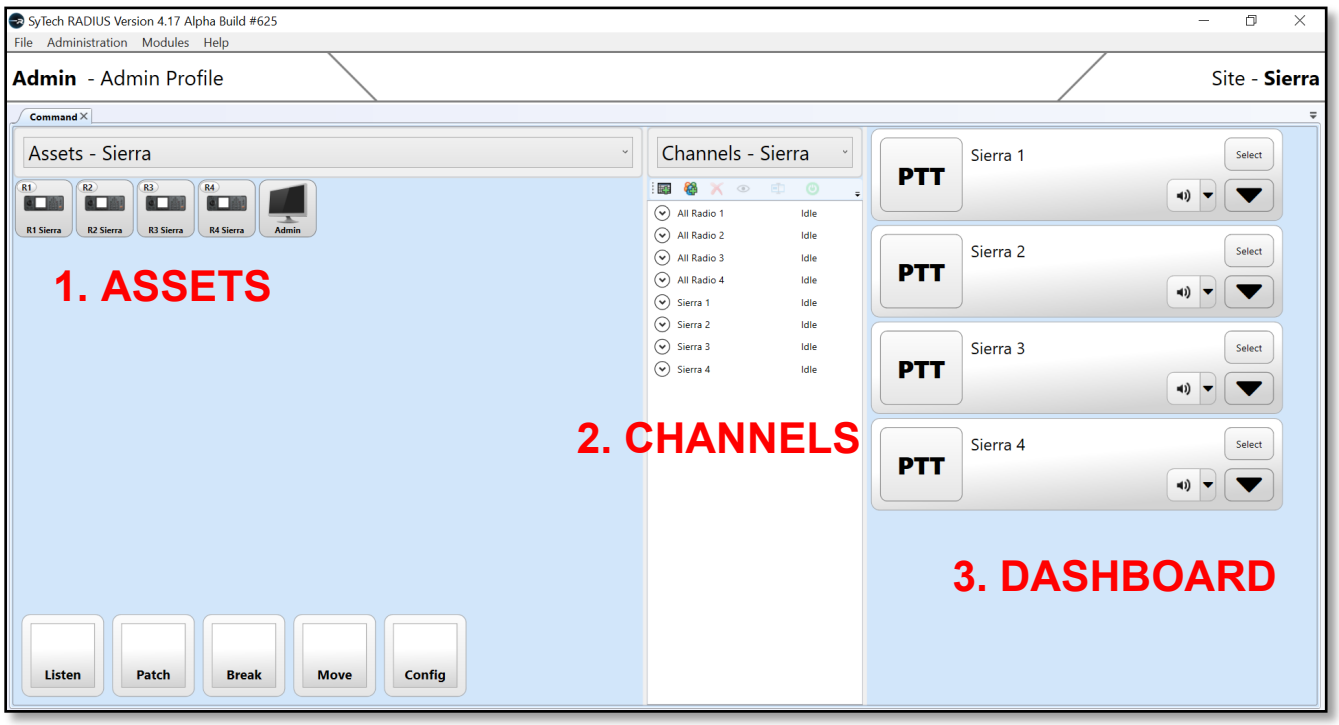
The RADIUS Client combines the functionality of the system administration tool with the capability of the end-user control software. By configuring the system for various uses, the system administrator can configure the graphical user interface to meet the needs of various end-users.

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

1. The application title bar. The RADIUS Client Version is indicated.
2. **The Menu Bar** is presented. It contains a variety of high-level commands for system usage. For example, the File, Administration, Module, and Help are found in the Menu Bar.
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 opened, 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 and **functions** such as monitor, patch, and control. The user can create patches among assets and 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. Its purpose is to simplify push-to-talk functionality.

3. **The Dashboard Module**: Allows the end user to access the channels the administrator created easily.

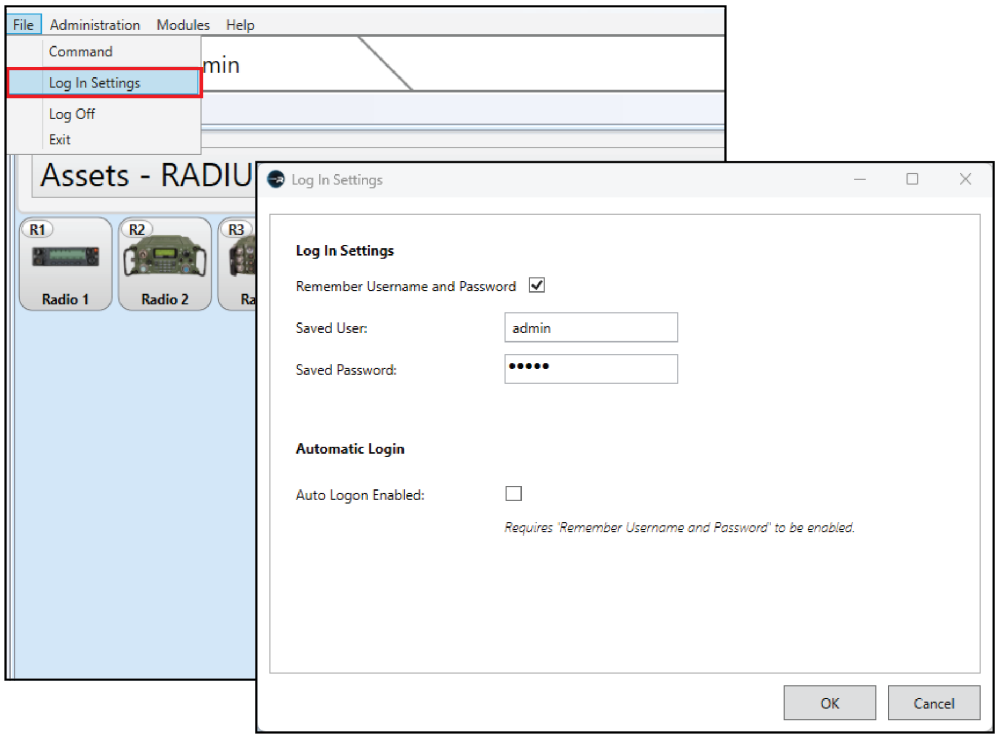
Quick Tip: The user can zoom in and out to resize the graphical user interface using "CTRL + scroll" on a keyboard and mouse, or by pinching in and out on a laptop touchpad. The zoom in/zoom out feature is also available for resizing the virtual control heads.

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

3.4 Login Settings

The Log In Settings menu allows the operator to configure saved credentials and automatic login behavior for the RADIUS Client.

To access Log In Settings, select File from the menu bar, then choose Log In Settings.



The following options are available:

- Remember Username and Password – When enabled, the RADIUS Client stores the entered User ID and password. The saved credentials will automatically populate the login fields on future launches.
- Saved User – Displays the stored username. This field is editable when the “Remember Username and Password” option is enabled.
- Saved Password – Displays the stored password in masked format. This field is editable when the “Remember Username and Password” option is enabled.
- Auto Logon Enabled – When enabled, the RADIUS Client will automatically log in using the saved credentials upon application startup.

Note: The “Auto Logon Enabled” option requires that “Remember Username and Password” is enabled. If credentials are not saved, automatic login cannot be performed.

After configuring the desired settings, select OK to apply changes. The RADIUS Client will need to restart to save these changes.

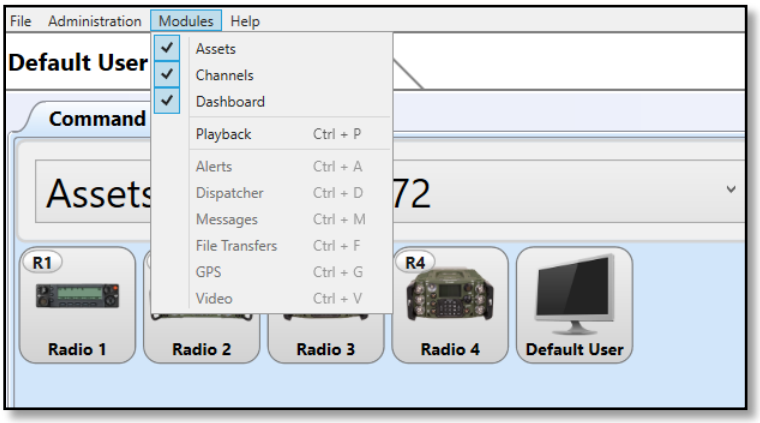
4. RADIUS SYSTEM MODULES

RADIUS System Modules represent the functional components available to the user within the client interface. By default, RADIUS includes three core modules: Assets, Channels, and Dashboard.

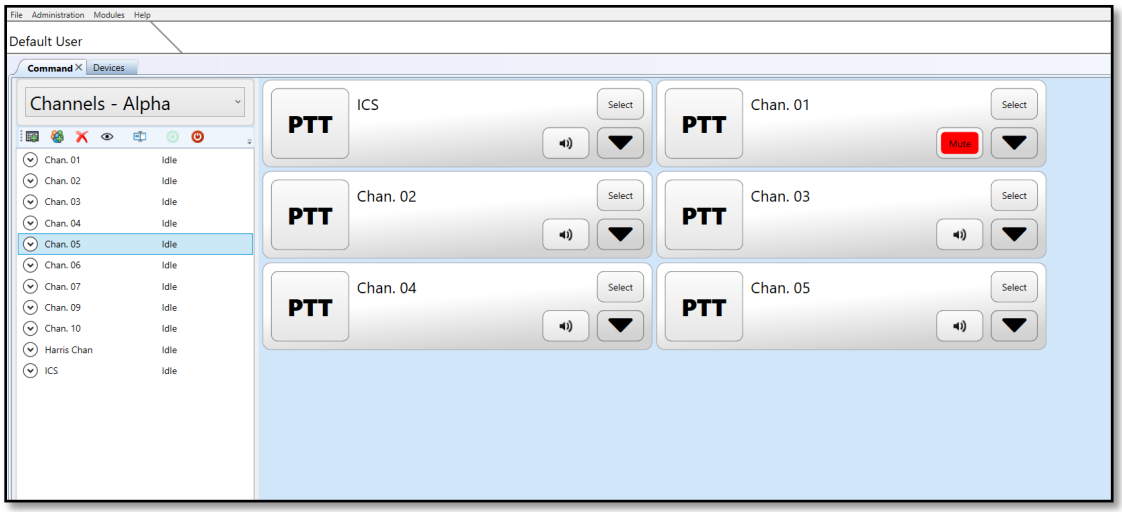
Select Modules from the menu bar to view the available modules. The drop-down menu indicates the status of each module as follows:

- Checked – Module is currently active.
- Black text – Module is available but not currently selected.
- Gray text – Module is not licensed or not available.

If the system is licensed for a module and the user has the appropriate permissions, the module can be selected and enabled from this menu.



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



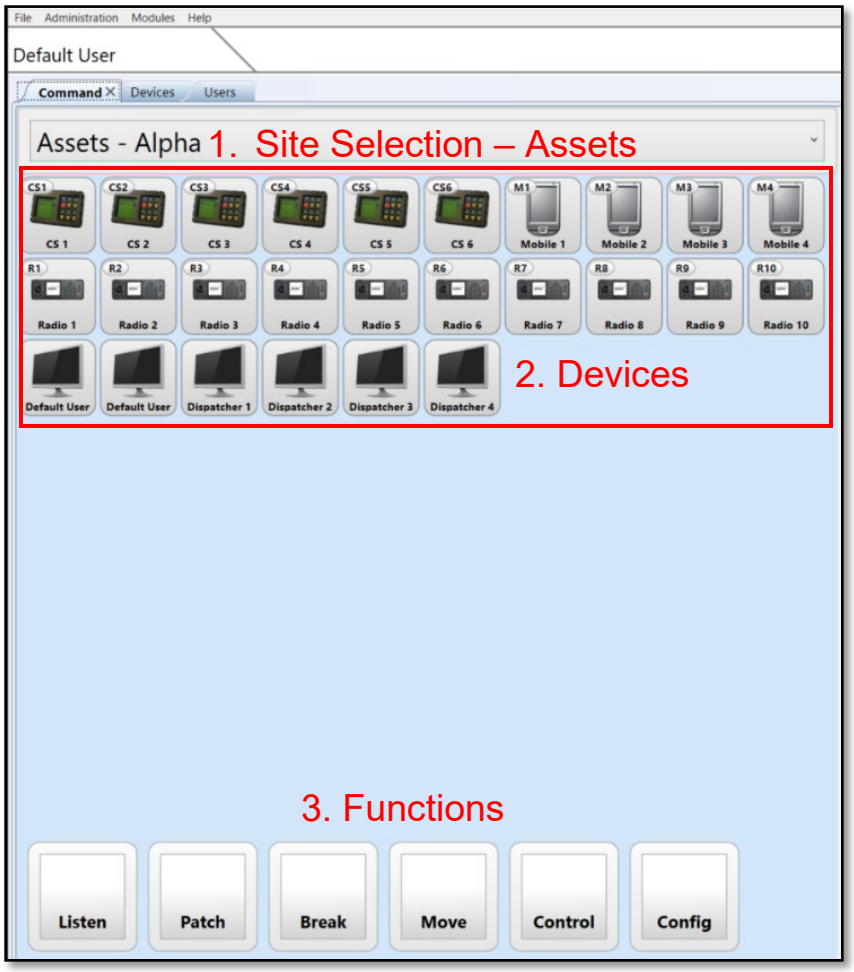
The following section outlines the capabilities and operation of the various RADIUS modules.

4.1 The Assets Module

The Assets Module graphically represents the available devices and functions available to the user. If permissioned, 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 – Asset**s: 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 granted permission to use the function, the corresponding function button will not be shown.



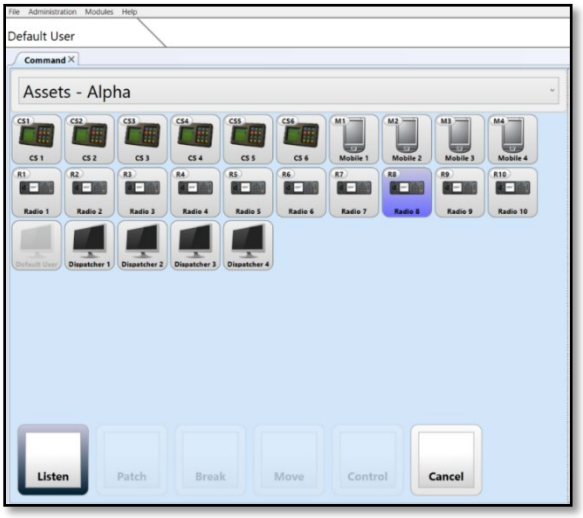
4.1.1 Listening to a Device

Monitoring a receiving radio can be performed using the Listen function by selecting the desired radio. In the example below, Radio 8 is receiving audio, as indicated by the green highlight.

In many system configurations, the Listen function is not enabled, as it may be redundant with the Mute/Unmute functionality available within a channel.

To listen to the receiving radio:

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



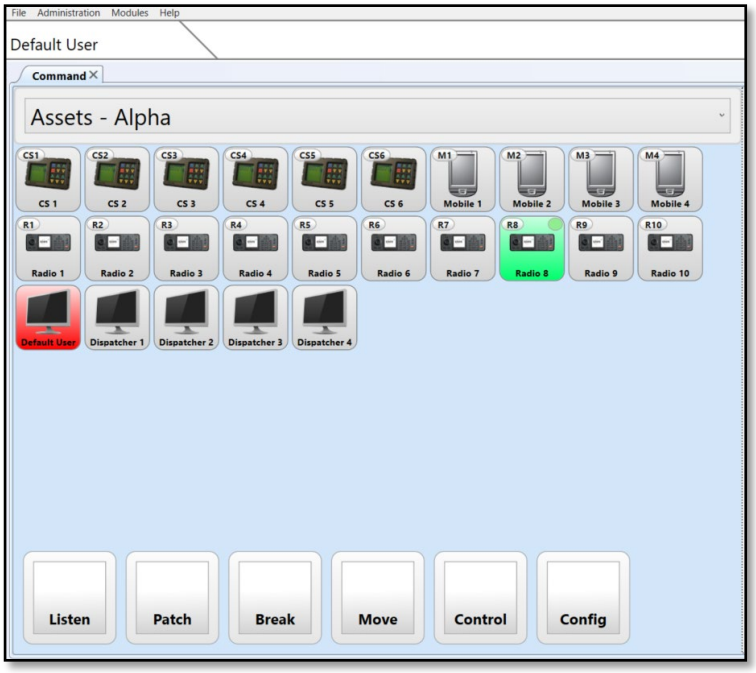
3. Confirm the selection by deselecting the Listen function.

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 device or channel is receiving audio

Red: The device or channel is transmitting audio

Note: Indicators reflect the perspective of the selected device or channel, not the user.



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.

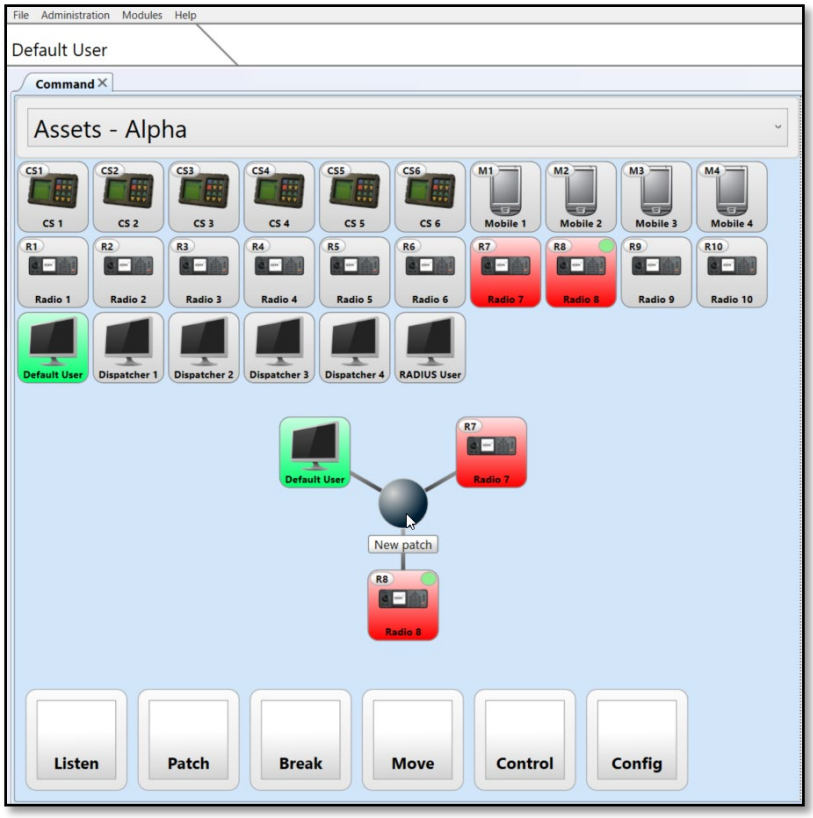
3. Finalize the patch by re-selecting the Patch function.

   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 be re-select the Patch function. The devices will be added.

4.1.6 Renaming a Patch

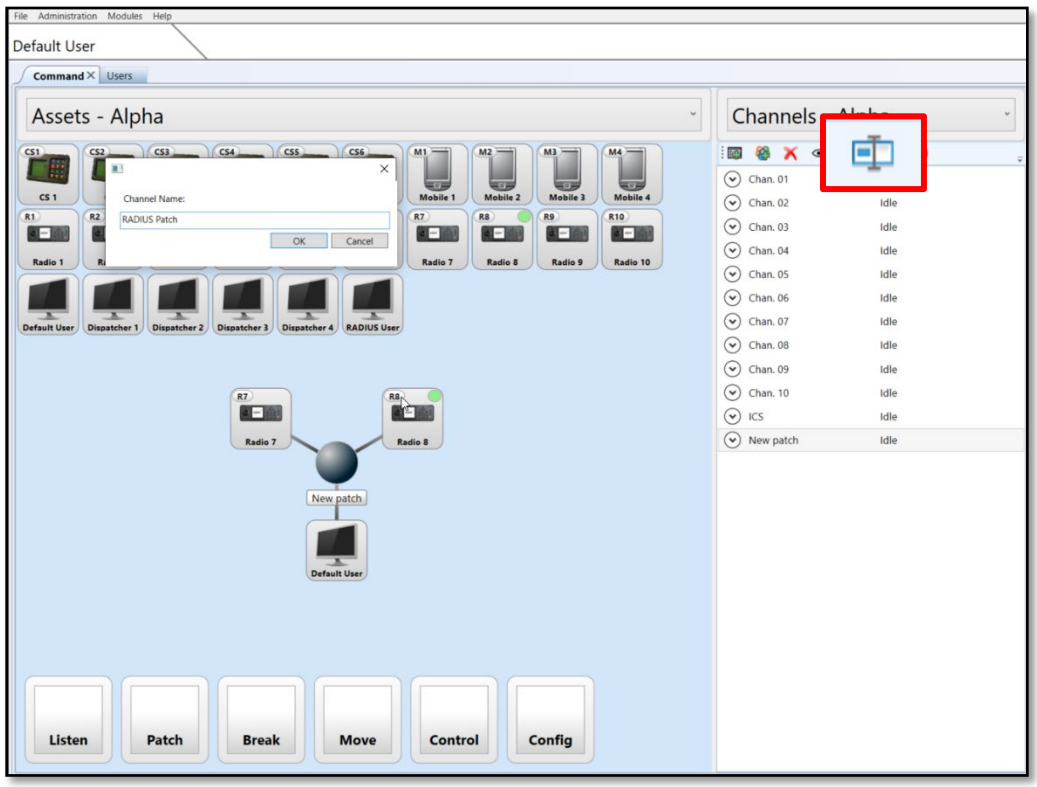
Renaming the patch can be accomplished by utilizing the Channels Module. When a patch is created, it is automatically added to the Channel Module.

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 enables administrators to view, create, and modify system **channels** within RADIUS. Channels are semi-permanent nets created by the administrator. Channels may include any 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, the recommended practice is 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 permission is granted, any device can be added to a channel. The device may exist in multiple channels simultaneously.

4.2.1 Viewing and Communicating to a Channel

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

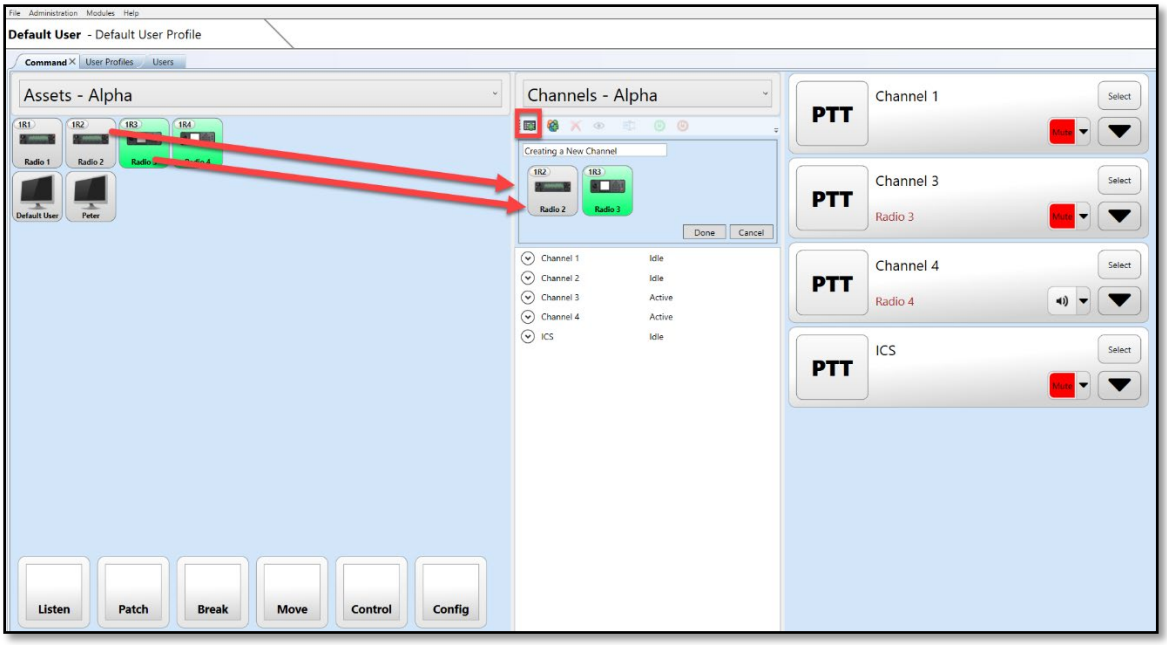
The "Show" icon may also be used to view the channel within the Dashboard.

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. The channels are alphabetized within the list. The user can view a channel by double-clicking on it 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

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

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 a 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 be disabled and no longer available for selection.

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.

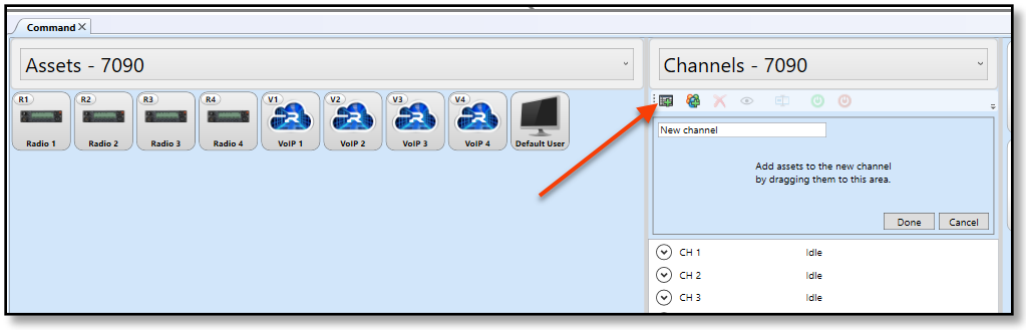
4.2.8 Channels within a RADIUS Multisite

RADIUS MultiSite allows the administrator to create channels that include assets from more than one connected site. This enables users to group local and remote devices into a single channel for monitoring and communication.

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

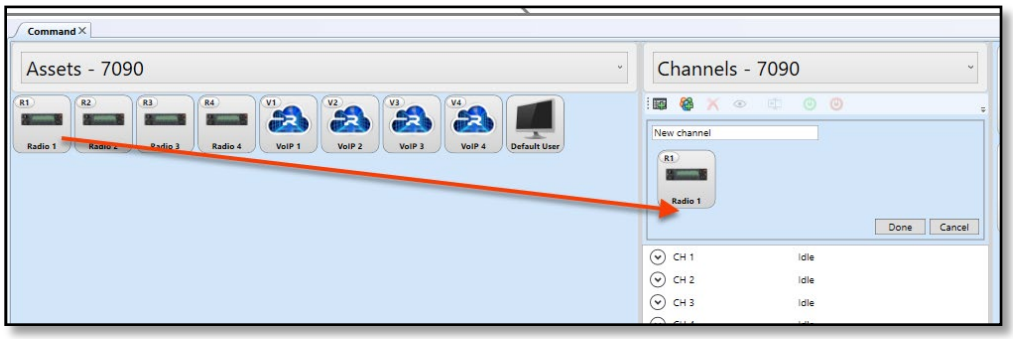
To create a MultiSite channel:

1. In the Channels module, select the Add Channel icon.

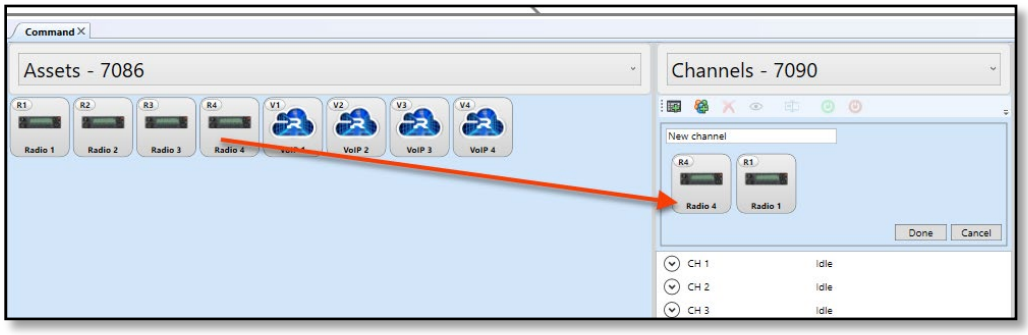


2. In the Assets module, confirm that the local site is selected in the site drop-down menu.

3. Select and drag the desired local asset into the “Add assets to the new channel” window in the Channels module.



4. In the Assets module, select the remote site from the site drop-down menu.

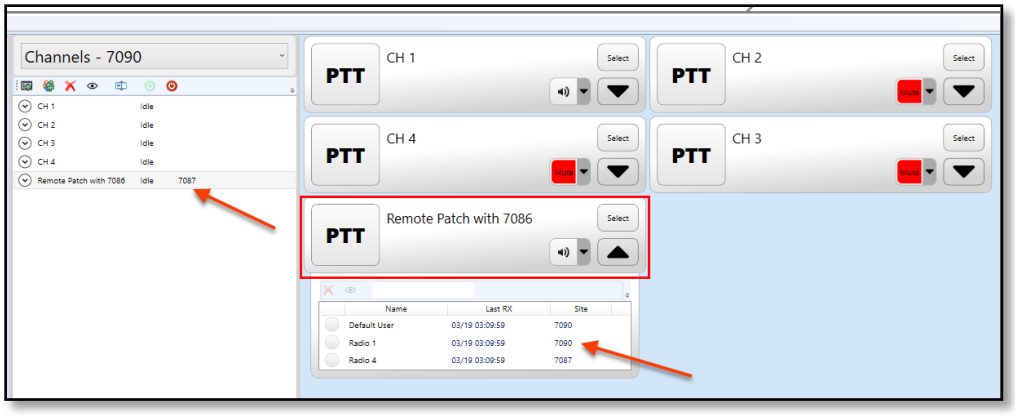


5. Select and drag the desired remote asset into the “Add assets to the new channel” window.

6. Verify that both the local and remote assets are shown in the new channel window.

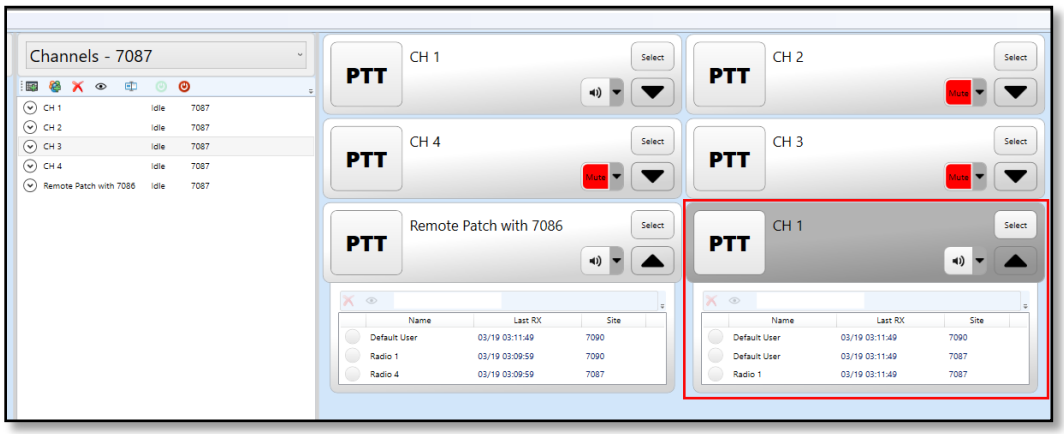
7. Enter the desired channel name.

8. Select Done to create the channel.



The new MultiSite channel will be added to the Channels list and can be displayed in the Dashboard like any other channel. Channels that include remote assets are indicated in the Channels module. From the channel drop-down in the Dashboard, the operator can view channel participants and the associated site for each asset.

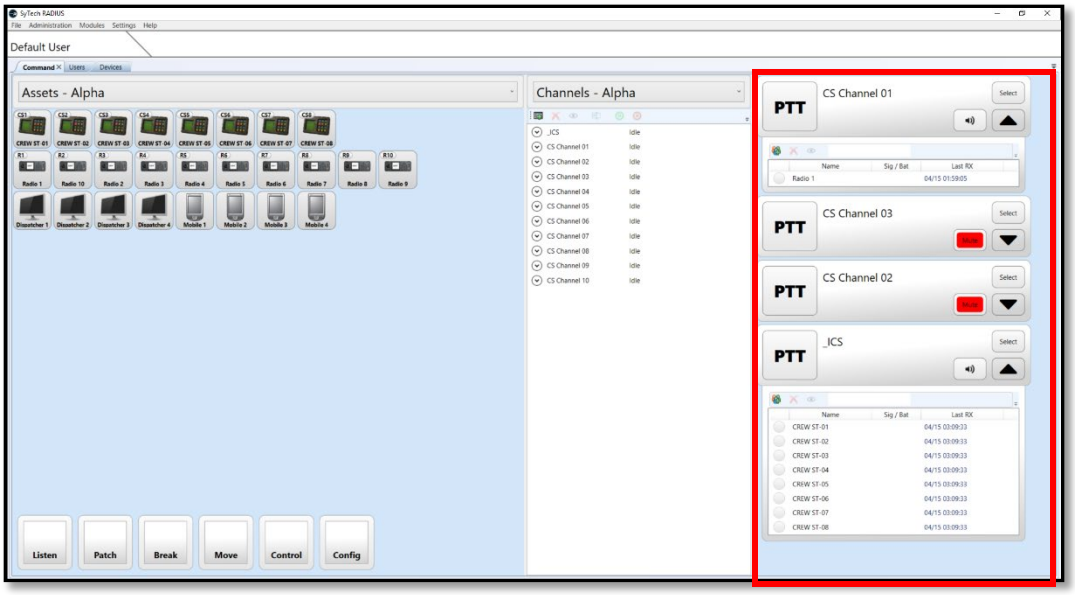
To monitor a remote channel, select the site from the channel drop-down and double-click the channel. The channel will be displayed in dark gray.



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. When the PTT button is pressed, the channel will illuminate green to indicate it is receiving audio from the user.

When receiving audio on the channel, the audio's originator 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.

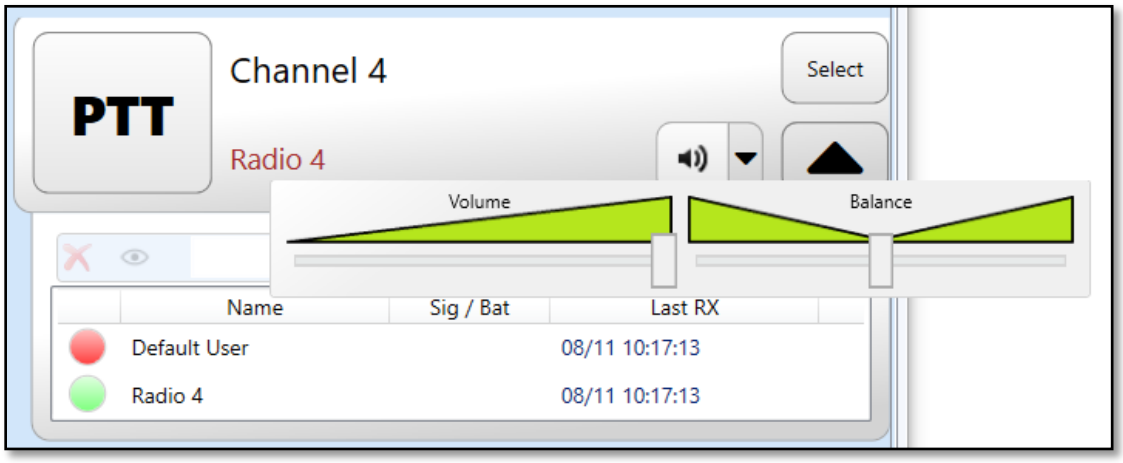
A green or red indicator will be illuminated adjacent to the respective participant when receiving or transmitting audio within the channel.

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 enables 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.

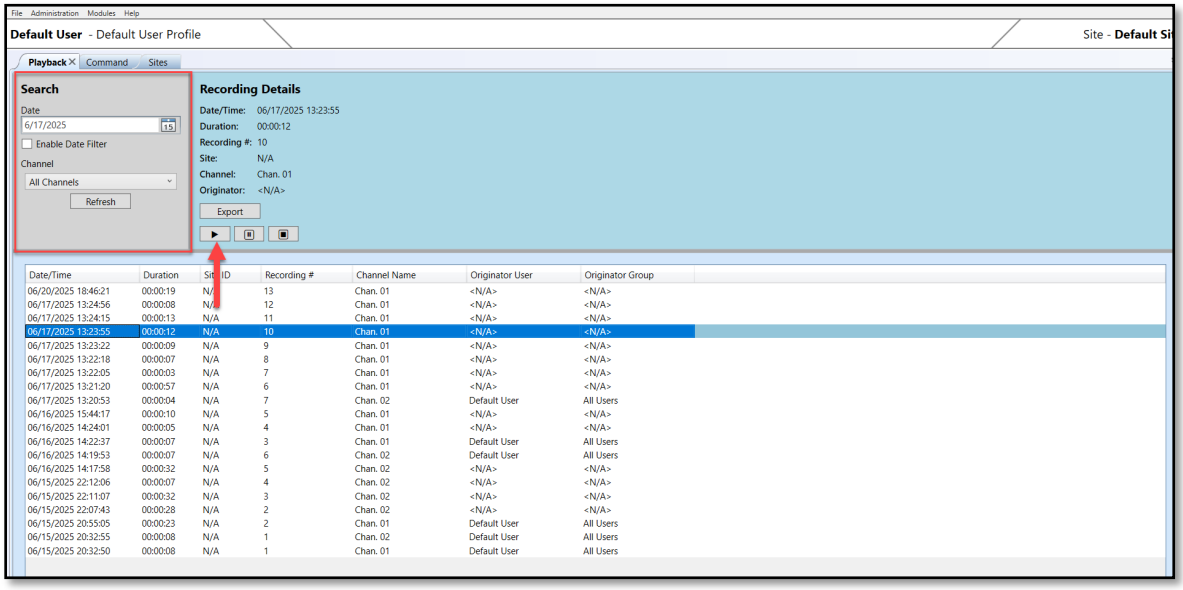


4.4 Playback Module (Optional License)

RADIUS offers a recording and playback module as an optional feature for its systems. If licensed for Playback, select “Playback” from the Modules menu in the menu bar. The Playback interface will be displayed as shown below.

Select the Refresh button to query recordings. If necessary, the operator can search for recordings by date or channel.

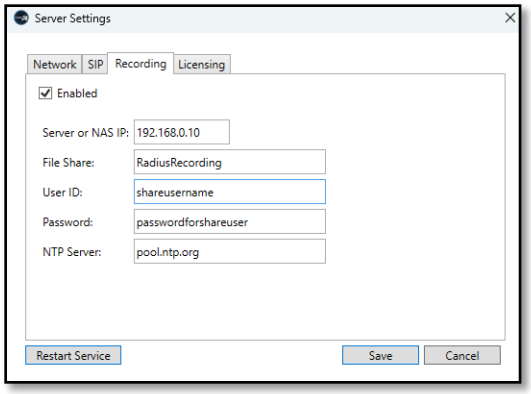
Select the recording to be played back. Then select the “play” button. The recording can be exported as a .WAV file using the “Export” button. Pertinent information is shown in the Recording Details.



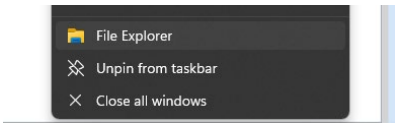
RADIUS stores the recording via a file share as configured from the “Change Server Settings” in the “Administration.” Standard Windows configurations for the file share are required.

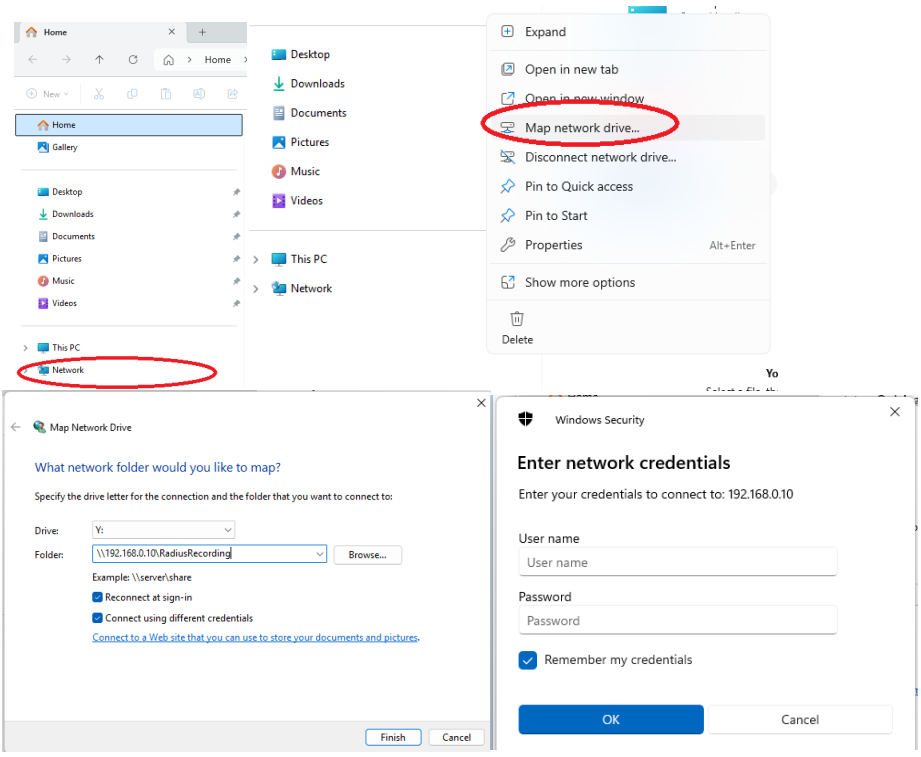
4.4.1 Configuring a Storage Location

RADIUS stores the recording to a network location, either a Server or NAS that can be specified from the Server Settings Menu. The RADIUS DS will need Read/Write permissions to this location. This is accessed from the Administration Menu, under the “Change Server Settings…” selection, then selecting the “Recording” tab.

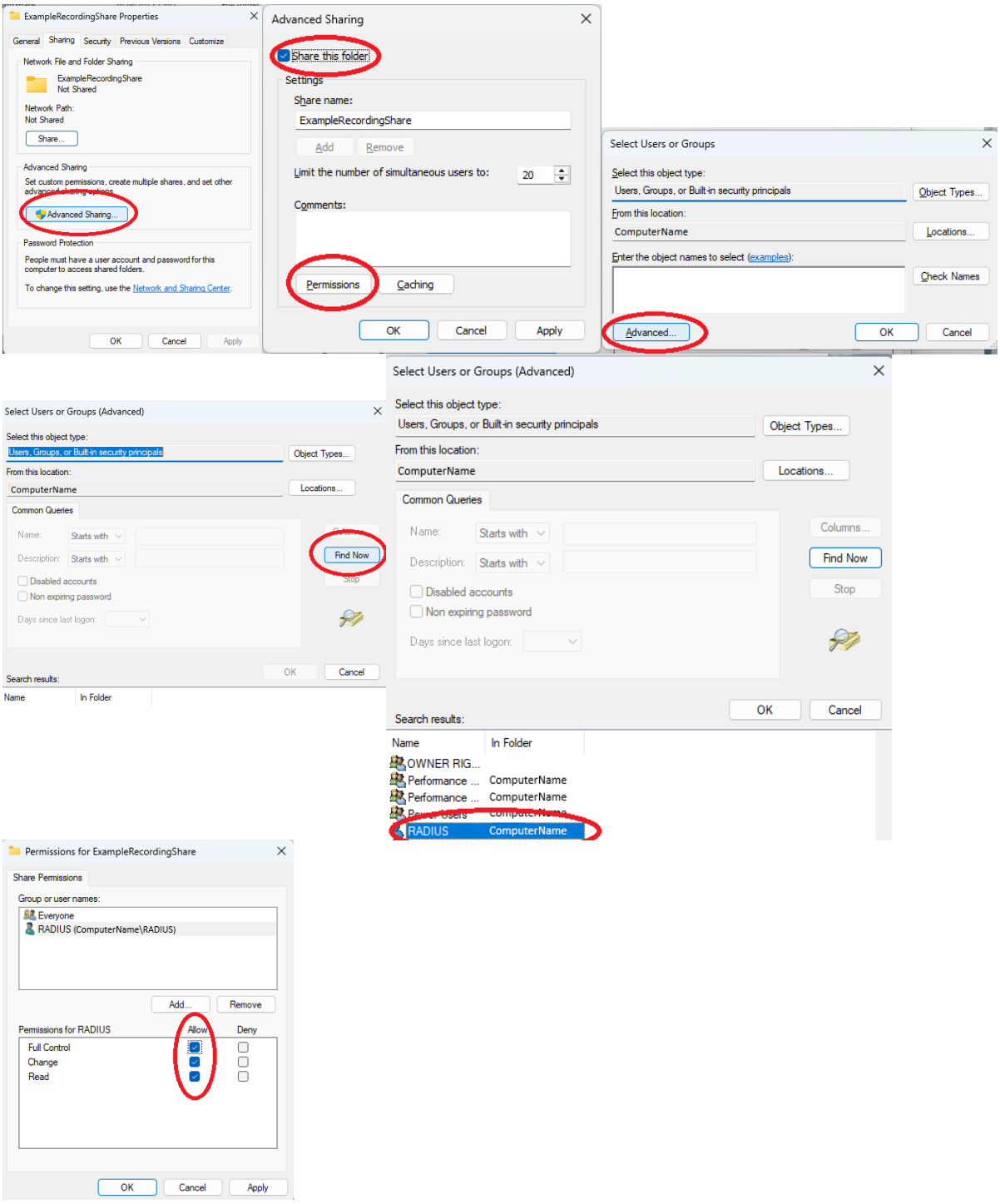


For the RADIUS client Windows application to have access to the recordings, it must also have access to this location. (Read Permissions). The images below outline this process.





Setting up a Network Share on a Windows Machine:



The RADIUS Server will need a User with “Full Control”, “Change” and “Read” of the Share location. The RADIUS Client will just need “Read” Permissions to the Share Location.

4.4.2 Network Time

RADIUS requires access to a network clock to apply time to the audio recordings accurately. If the recordings indicate an incorrect time, the DS time is not correctly synced.

To Configure the DS Time

1. Select Administration
2. Select Server Settings
3. Select the Time tab. RADIUS offers multiple ways to associate a time source with the DS. If a network time service is present, the administrator may choose to “Use Time Server.” Configure the third-party device, such as a Windows PC, router, or time server, and enter the device's IP address. Select “Sync Now.”

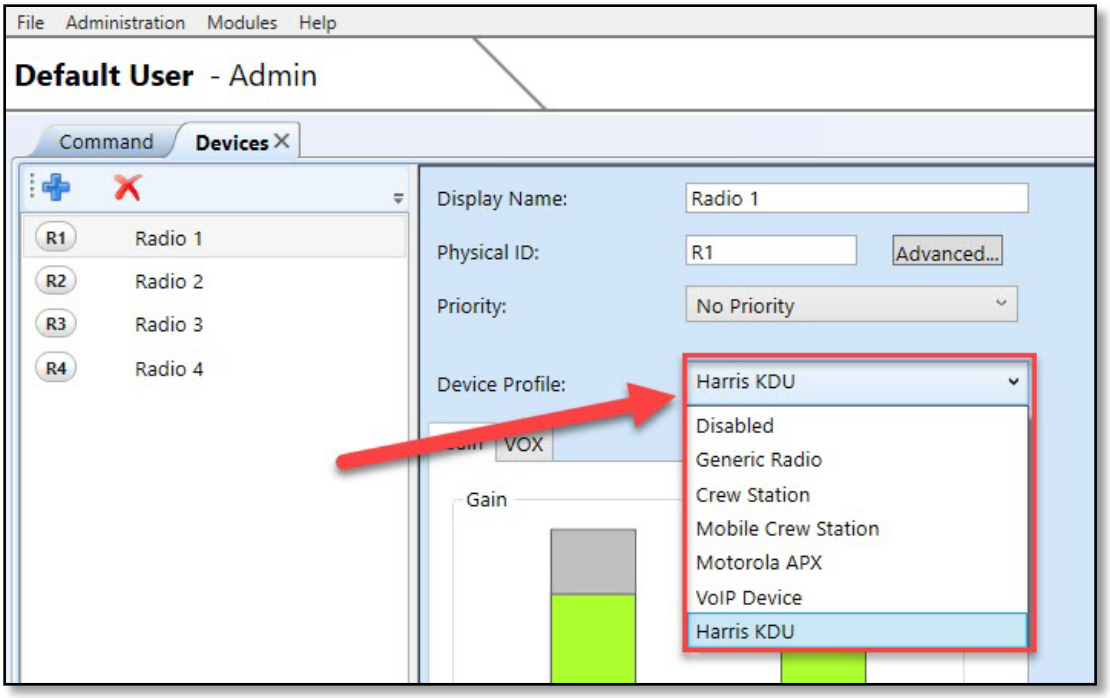
   If a third-party device is not available, the administrator can sync the DS time to the Windows client as a temporary solution. To do this, select “Sync Server Time to Client Time.”

   A time server is the recommended approach to supplying time to the DS. By accessing a third-party device during the boot process, the DS will have the correct time without administrative assistance.

4.5 Remote Radio Control and the Virtual Control Head (Optional License)

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

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



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

4.5.1 Accessing Remote Radio Control

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

   On the following page, an image shows a VCH for the Harris KDU. The controls for the KDU VCH are labeled on the image and described below.

Display Name: The name displayed in "Display Name" is found in the Device Editor.

Display Screen: Information from the radio will be displayed here.

Push-to-Talk: Enables the user to PTT to the radio. When engaged, the PTT button will light up green (indicating that the KDU is receiving audio). When the radio is *receiving* audio, the KDU will light red (indicating it is emitting audio). After a reception, the PTT button will flash yellow for five seconds.

Audio Control: Enables the user to mute and pan the audio level and balance. Note that when the control head is first opened, it is muted by default. 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 the next time the RADIUS client is reopened.

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.

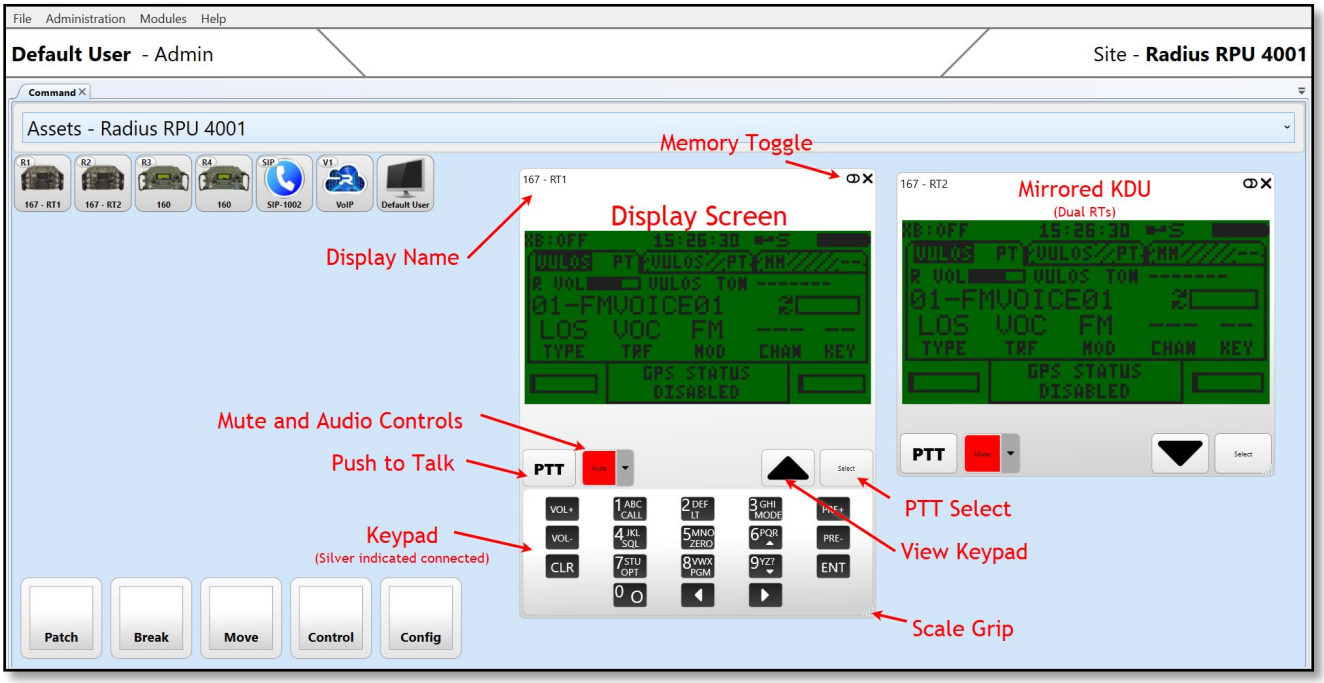
Keypad: Provides the available button controls to the user. When the keypad appears pink, RADIUS does not sense the radio. When the radio is correctly connected, the keypad will turn light gray. The pink background color indicates that the radio is not communicating with the gateway.

Keypad Control: Opens and closes the keypad.

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

Scale: Enables the user to rescale the VCH.

Close: Closes the VCH.



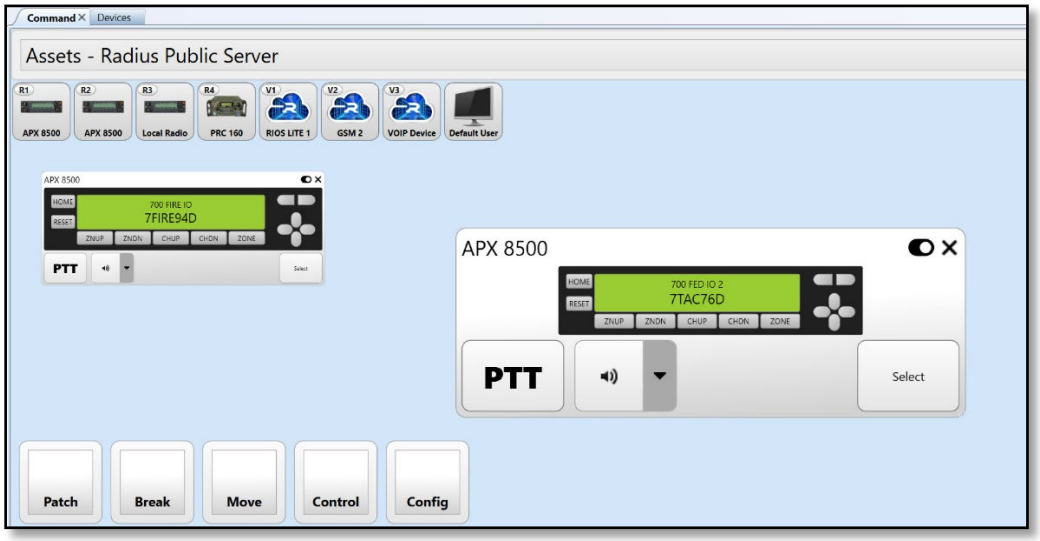
4.5.2 Virtual Control Head Scaling

Two controls exist for scaling the virtual control head.

1. The scale handle is located at the bottom right of the virtual control head (see above). This control modifies the control head's length and height.

2. On the keypad, hold “CTRL” and roll the mouse wheel when the cursor is over the virtual control head. This controls the ratio between the control head and the VCH buttons.

The image below shows two Motorola APX Virtual Control Heads. The VCH on the left is scaled down (handle dragged in) with a large radio image (CTRL/wheel rollback). The image on the right is scaled large (handle dragged out) with a small radio image (CTRL + wheel forward).



4.5.3 Additional Remote Radio Control Tips

Layering: The user can set the VCHs to layer over 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 models and cables include:

Motorola O5 and E5: CAB-00209B
Harris 117G: CAB-00273
Harris 160: CAB-00273
Air Avionics AC-1: CAB-00AC1
L3Harris ROX: CAB-00277 (See addendum to this manual)

5. RADIUS ADMINISTRATION

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

The significant portions of the Administration tab include:

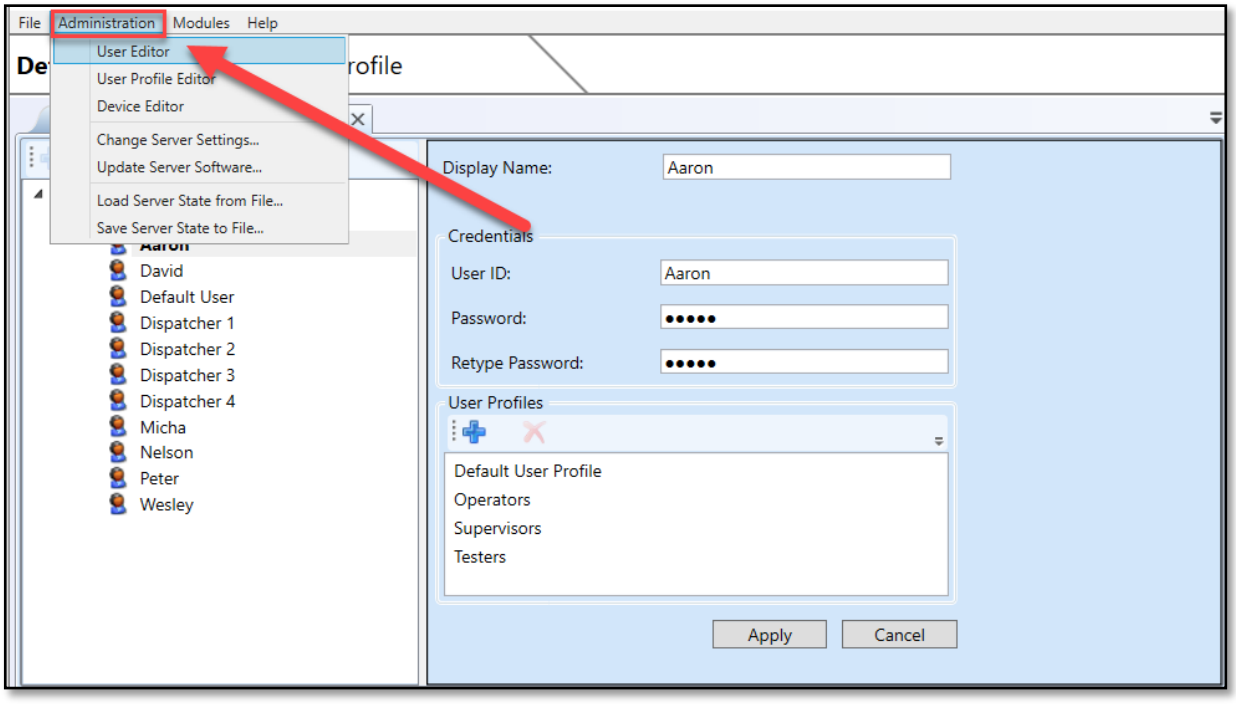
- **User Editor**: Allows administrators to create user names and passwords and assign users to User Profiles.
- **User Profiles**: Enables administrators to create User Profiles. User Profiles can be thought of as “access templates” for user groups.
- **Device Editor**: Enables administrators to modify and add devices, including 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 and highlight other capabilities within the Administration tab.

5.1 User Editor

The RADIUS User Editor enables administrators to create users and assign user credentials. To access it, select the “User Editor” from the Administration tab.

The RADIUS User Editor will be shown below.



5.1.1 Creating a New User

To create a new user:

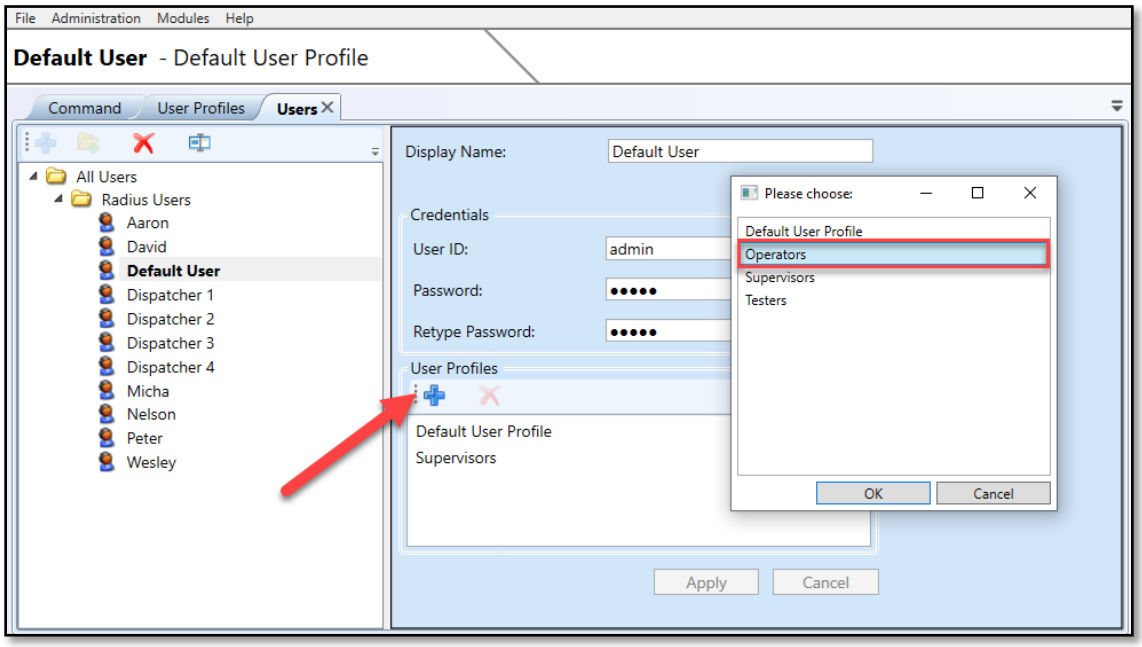
1. Select the group where the new user will reside.
2. Select the "+" icons to create the new user.
3. Input the desired Display Name, User ID, and password.
4. Select "Apply."

5.1.2 User Profile Assignment

The User Profile defines access to resources and system capabilities. The following section, titled "User Profile Editor," outlines how to create User Profiles. If User Profiles already exist, the administrator can assign users to a User Profile within the User Edit.

The administrator can assign the correct User Profiles in the User Edit.

The image below shows the administrator adding a User Profile to the "Default User." To add a User Profile, select the "+" symbol, and the available profiles will appear. Choose the desired profiles, then click "OK" and "Apply."

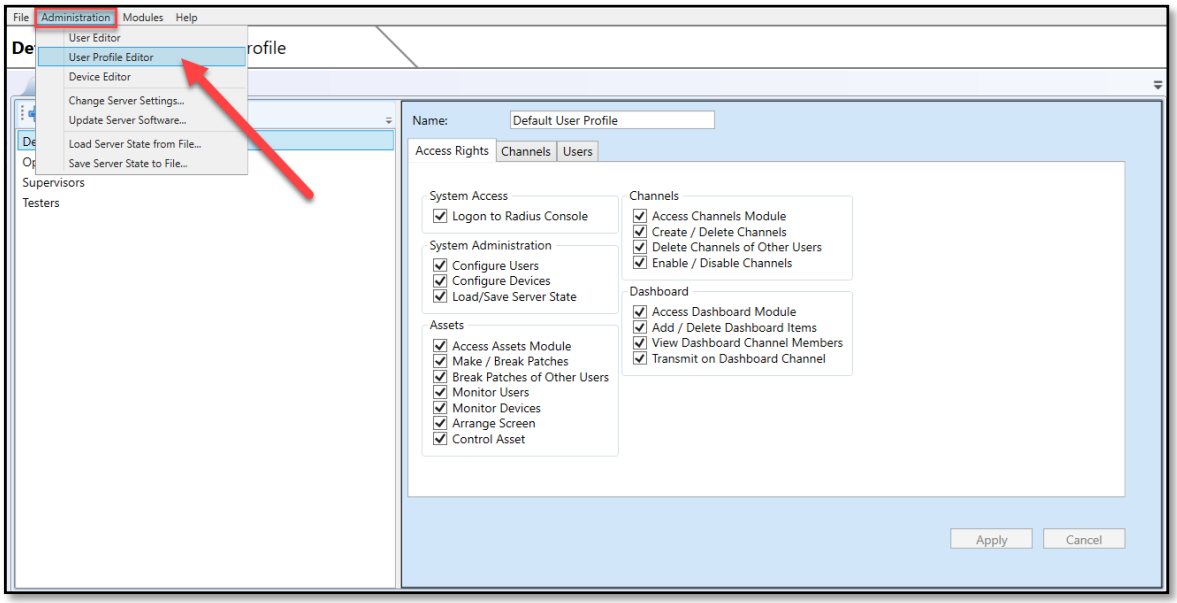


When the Default User logs in next time, they will be able to select the desired profile for login. User Profiles are explained in more detail in the following section.

5.2 User Profile Editor

The User Profile Editor allows the administrator to set access rights and channel availability for users added to the profile. User Profiles act as “access templates” for user groups created by the administrator. For example, in the example below, the administrator has created three additional User Profiles besides the “Default User Profile." These include “Operators," "Supervisors,” and “Testers.”

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



Within the User Profile Editor, these tabs control access 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: The User Profile can 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: Grants the User Profile permission to access the Channels module. If this right is not enabled, the user will only be able to view channels or functions within the Channels module, but not interact with them.

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 use the "Enable" and "Disable" functions in 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 channels or channel controls in the Dashboard module.

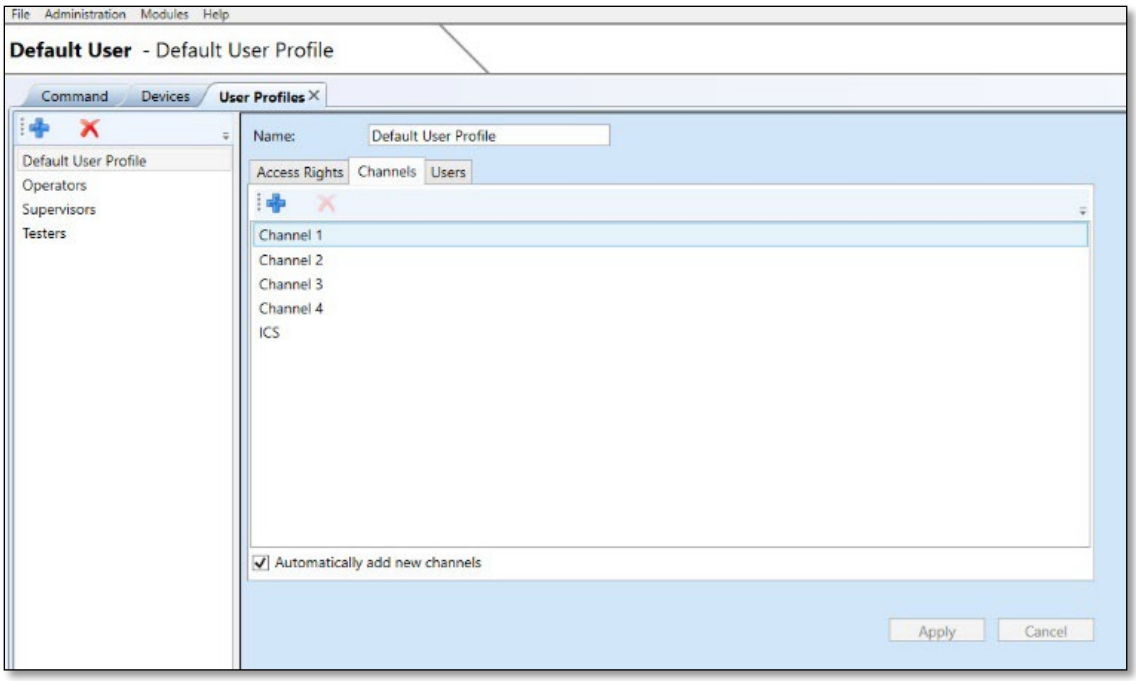
Add/Remove Dashboard Items: Allows the User Profile to add and remove items from the Dashboard by double-clicking channels in the Channels module.

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."

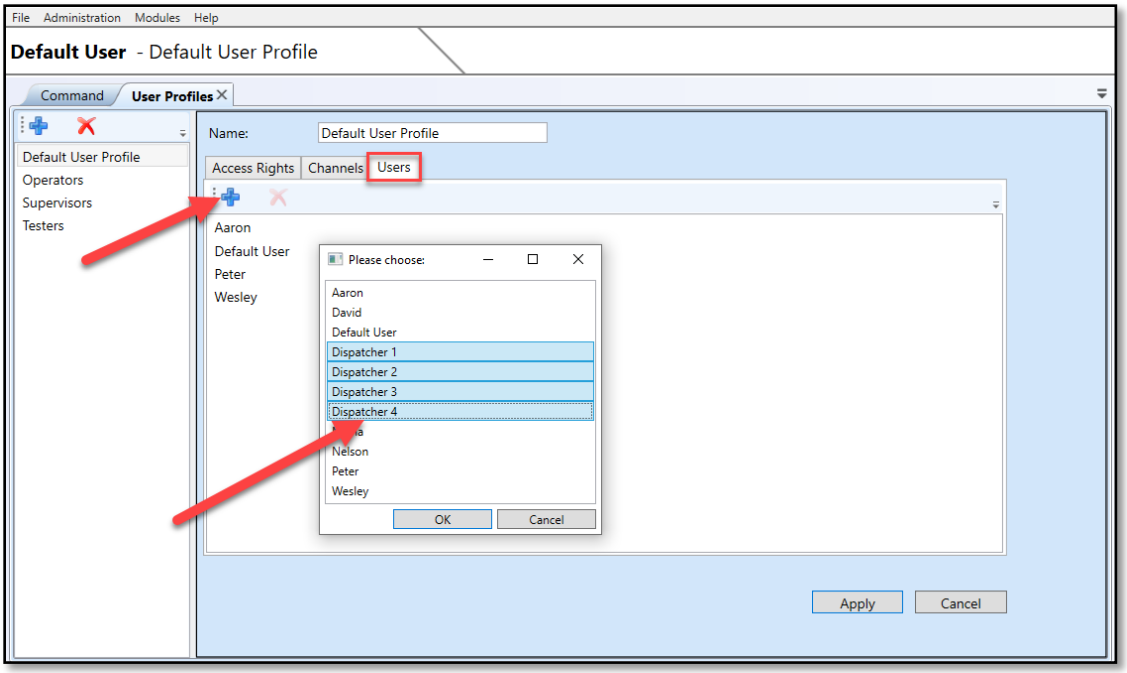


Note: The access right called “Automatically add new channels” allows users in the User Profile to see newly created channels and patches without needing to add them after creation. The default setting is enabled.

7. Next, click on the “Users” tab. Users with access to the User Profile are displayed.

8. To add users, click the blue “+” sign. Users created through the User Editor will appear. Select the new users to add them to the User Profile. Hold CTRL to select multiple users, as shown in the example below.

9. Select “Okay.” The users will be added to the User Profile. When the user logs in with the correct Username and Password, they can select the desired profile.



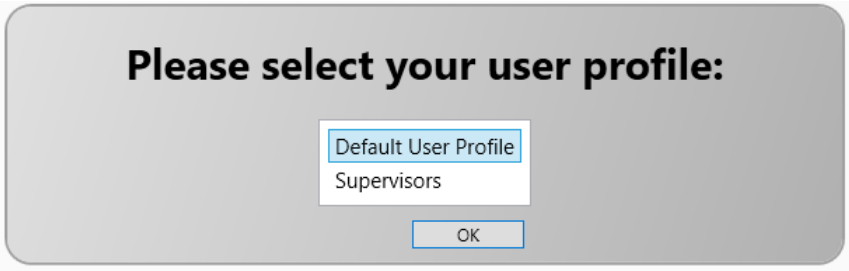
10. Select the “Apply” button.

    The User Profile has been created. It will now enforce the corresponding rights, channels, and users.

5.2.2 Logging in with a User Profile

If the user is assigned to more than one User Profile, the user can select a profile during login. If the user is registered with only one User Profile, the user will be automatically logged in to that User Profile.

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

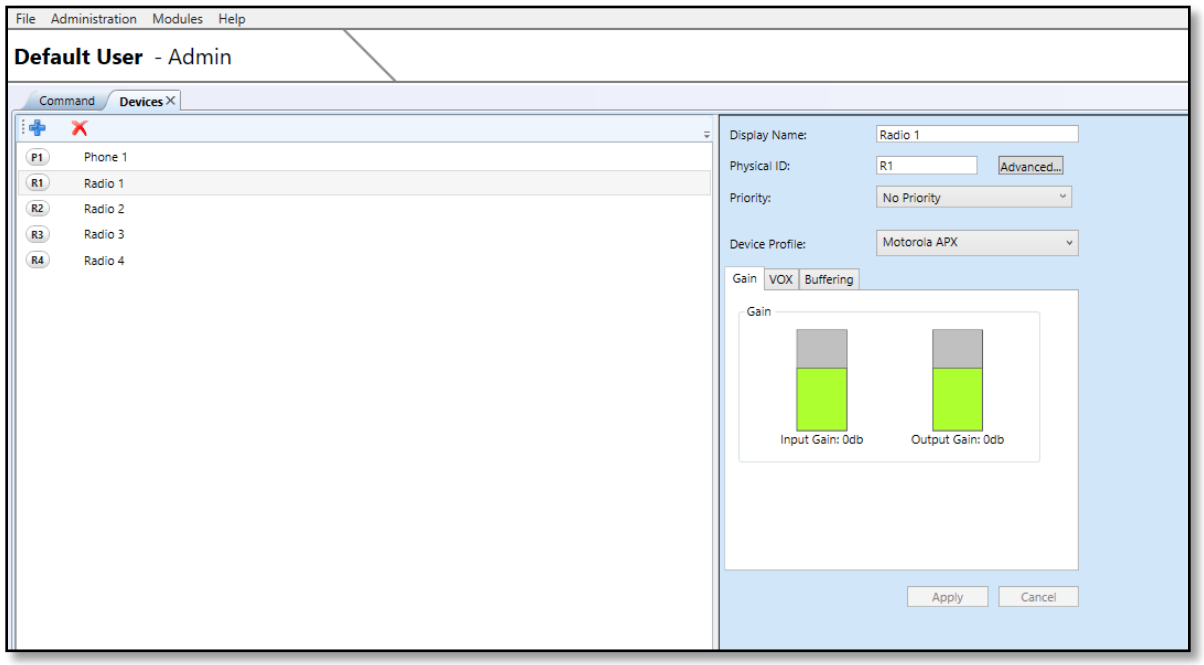


Upon selecting the desired profile, the user will now have access to the corresponding permissions and resources as created within the User Profile Editor.

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:



The existing devices are displayed on the left. The right-hand area contains the selected device configurations. In the image above, Crewstation #1 is selected. Device configurations such as Channel Assignment, PTT Button Mode, Microphone Gain, and others 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 that sorts the assets within the graphical user interface. Within the Assets Module, devices are sorted alphabetically by 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.

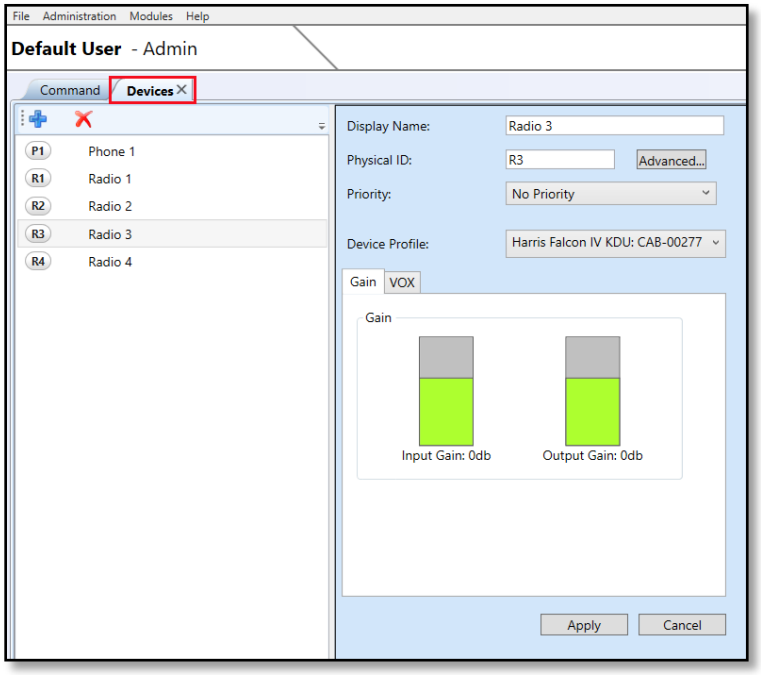
5.3.1 Radio Device Configuration

Radio Device Configuration refers to the configuration interfaces of a radio physically connected to the RADIUS DS. These configurations affect 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 radio device configuration 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 remain the same or be edited to determine the screen arrangement within the Assets Module. It 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 as follows: the preceding-priority device takes precedence over the latter. When the device is added to a channel, the priority is applied to the device within that channel.

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

5. **Credentials**: To enable radios to appear within the Command interface and provide port visibility on the LCD or status indicators, each asset must be configured with valid credentials. This procedure should only be performed if the ports have been deleted and must be recreated.

   By default, the Credentials field assigns a User ID in the format “rX,” where X corresponds to the radio port number. The default password uses the same value.

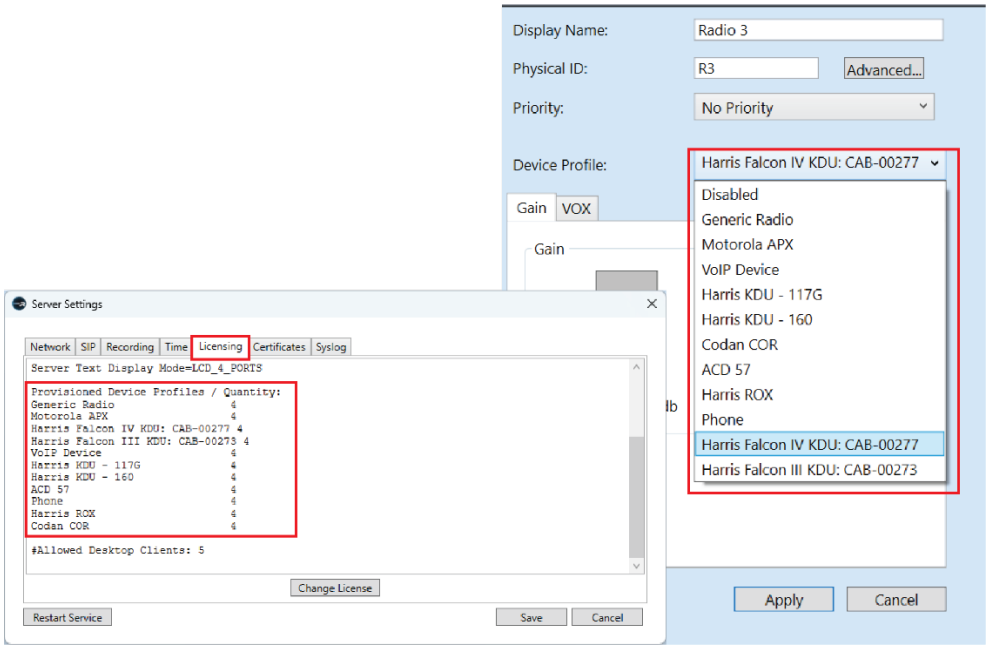
   For example, for port 15:
   - User ID: r15
   - Password: r15
   - Retype Password: r15

   After the password is applied and saved, the password fields will appear blank for security purposes.

6. **Device Profile**: The Device Type field allows the system builder or administrator to define the type of device being configured.

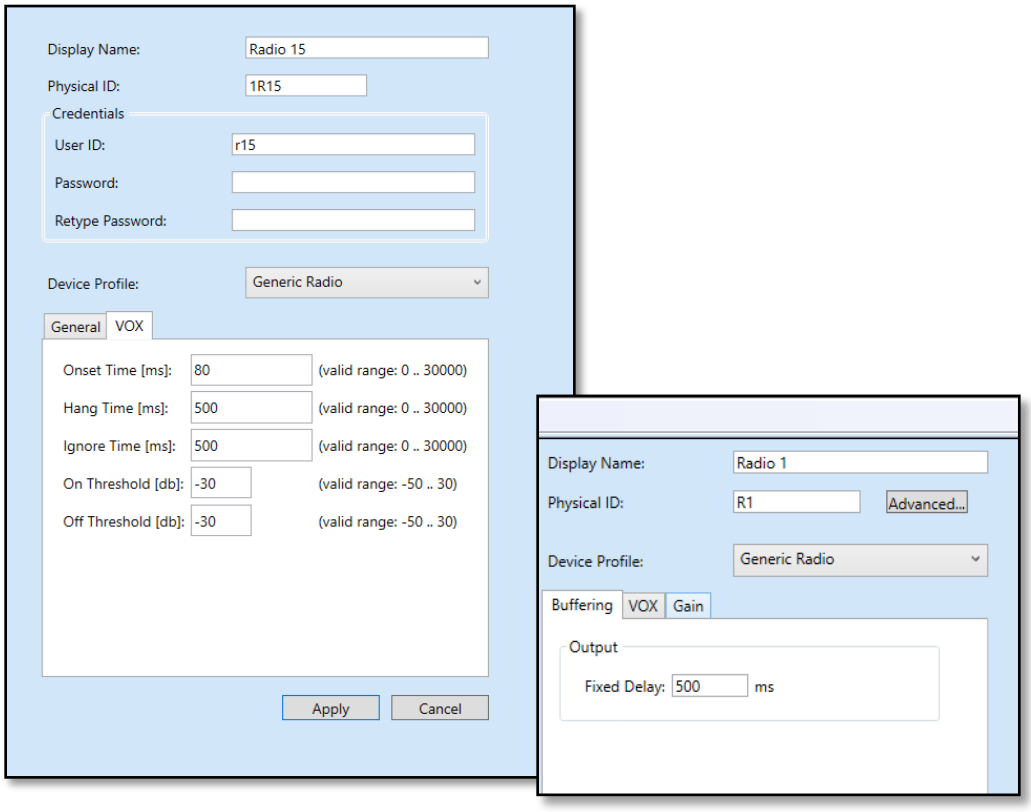
   The drop-down menu displays the available software profiles based on the system’s licensed device profiles. The list is automatically populated by querying the RADIUS license.

   In the example below, the operator has opened the drop-down menu. The available profiles correspond to those listed in the Licensing tab within the Change Server Settings menu.



7. **Gain**: Within the “Gain” tab, the user may modify the Input and Output gain by selecting the graphic. These settings are essential 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: In the Buffering tab, the administrator can set an outbound audio buffer to compensate for delays in audio transmission. This feature is recommended for trunking systems and PTT-over-cellular apps that require call setup time.

9. Select “Apply.” The radio device's settings will be saved.

5.3.2 Add a New Device to the RADIUS DS

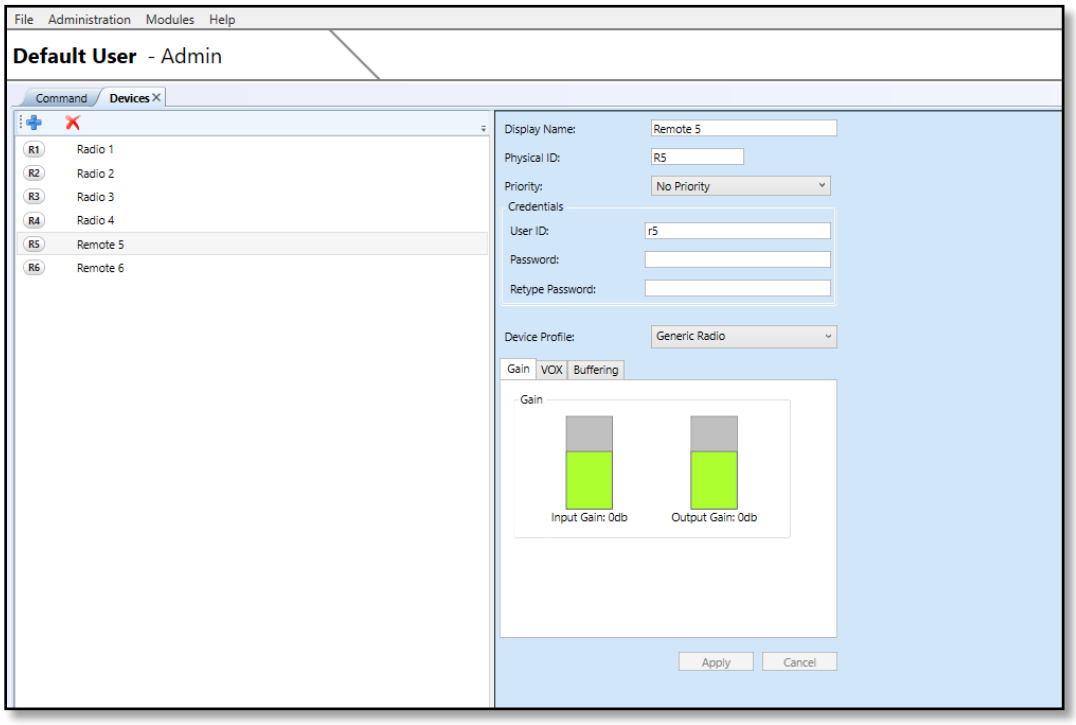
If a radio device is deleted, or if a new device (such as an nPoint or RIB) is added to the RADIUS Distribution Service (DS), the device must be added to the system before it can be used.

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 in to 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.” In the “Credentials” section of the configuration, use the User ID and Password configured in the previous step. For example, “r5” and “r5” for both fields.

   The image below is a new RIB titled “Remote 5” 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. Restarting the server after adding a new device is not necessary. If the RIB does not appear, restart the devices and confirm that all blue DS service lights are lit and the configuration is correct.

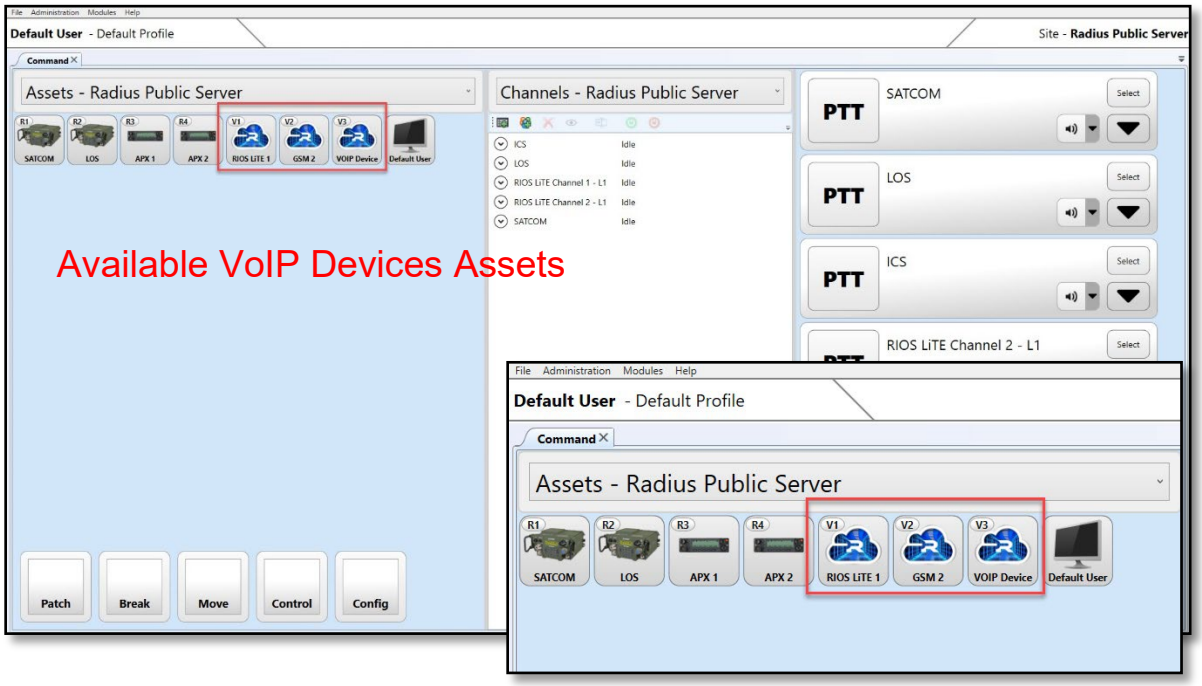
5.3.3 VoIP Devices

VoIP Devices in RADIUS refer to external devices that communicate 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, an ETC microphone, or a RIOS

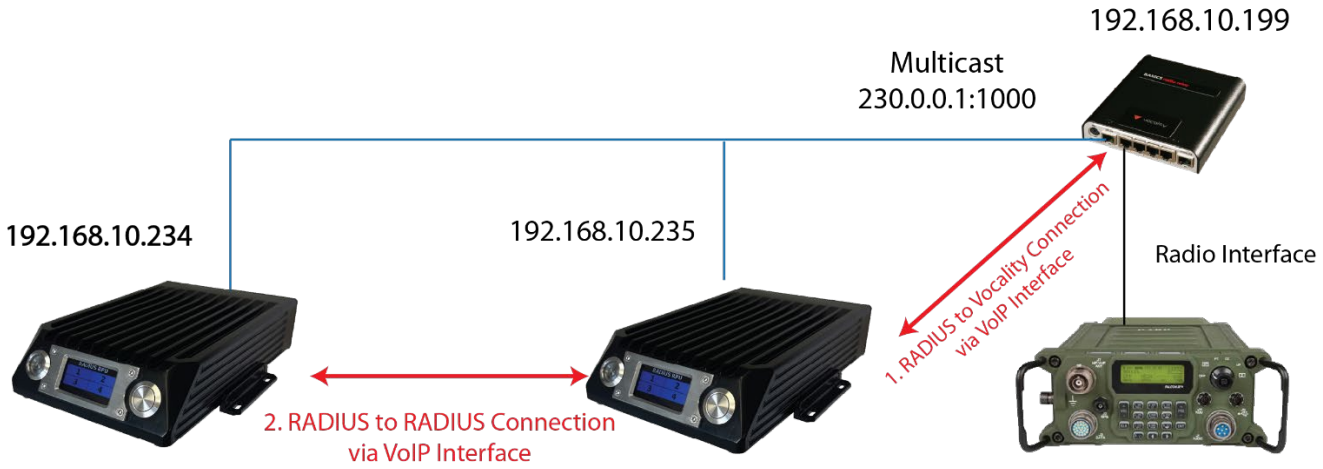
Server. The number of licensed VoIP Devices appears under the License Key in Administration > Change Server Settings > Licensing.

When a virtual device is added in the Device Editor, the RADIUS gateway creates an internal 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, allowing the operator to patch or place its radio on 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 communicates with a Vocality radio gateway and another RADIUS Gateway over an IP connection.



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 use a VoIP device to interoperate 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**.

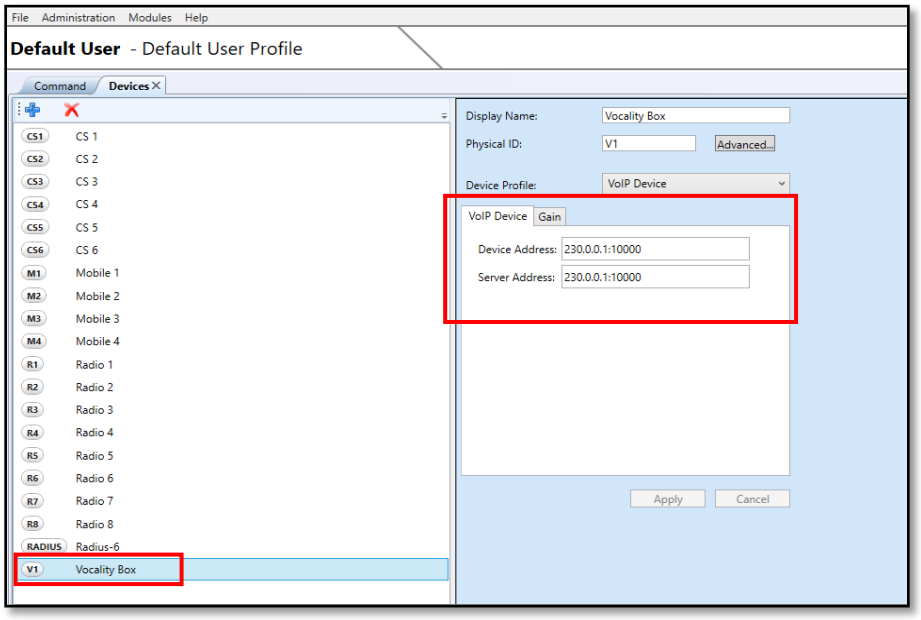
2. If a VoIP device is not already created, select the "**+**" sign.

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 address and port number are separated by a colon, with no spaces. This appears as:



5. Select "**Apply**." The VoIP Device will appear as a Radio Asset in 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.

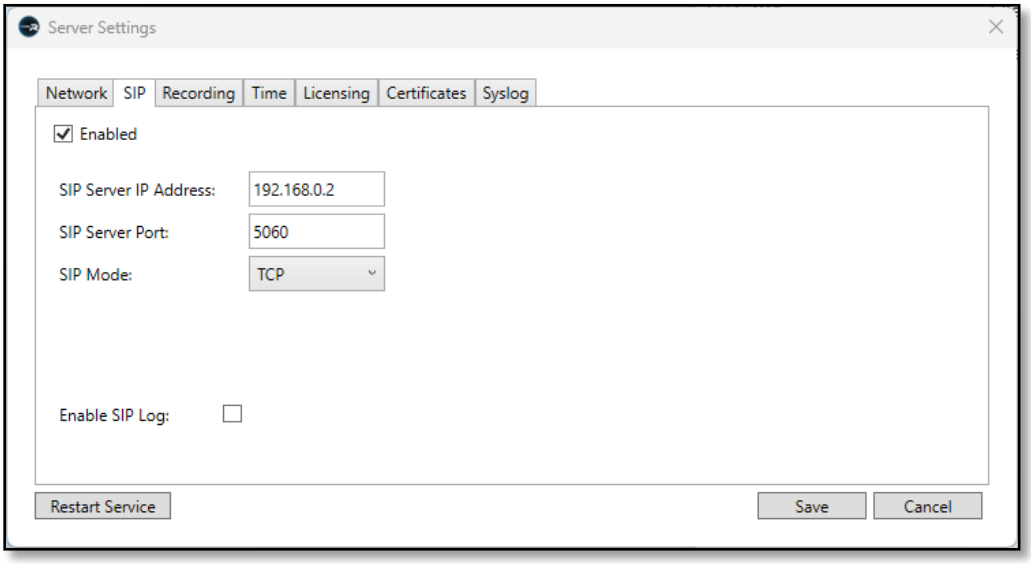
The operator can then patch or place the VoIP Device into a channel.

5.3.4 SIP Integration

If the RADIUS Distribution Service (DS) is licensed for the Phone Device Profile, the system can integrate and connect telephone assets using the Session Initiation Protocol (SIP).

To enable SIP:

1. Go to “Administration.”
2. Select “Change Server Settings.”
3. Select the tab for “SIP.”
4. Check “Enabled.”



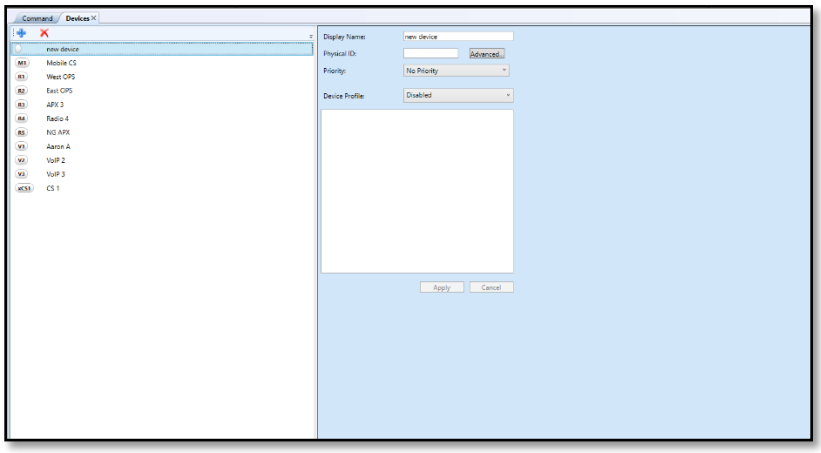
5. Input the settings for the SIP Server to be used
6. Click “Save.”
7. Restart the RADIUS server.

If the system is licensed for SIP Devices, the administrator can create SIP Devices that appear as assets in the Command tab.

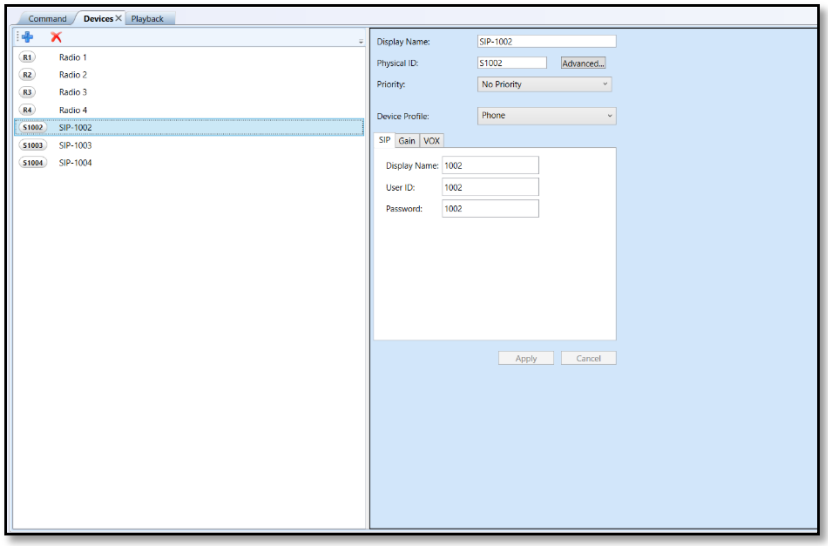
To Create a SIP Device:

1. Go to Administration.

2. Select Device Editor.
3. In the new tab, click the Plus Icon. 
4. Select “new device” from the list.

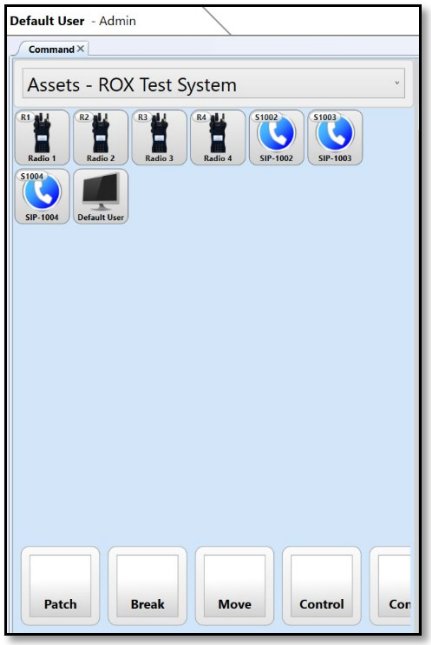


5. On the right side, select “Phone” from the *Device Profile.*



6. On the SIP tab input the information for the extension to be used by the device.
7. Display Name and Physical ID can be anything.
8. Once done hit the “Apply” button at the bottom of the screen.

After it has been applied, click on the command tab.



RADIUS represents the SIP assets as phone icons in the Command tab, as shown above.

<u>To Access the SIP Keypad</u>:

To access the number pad for the SIP Device.

1. At the bottom of the screen, click on “Control.”
2. Select the SIP Device you want to use.

Once the screen is up, it should look like the image below.

When using the SIP, the user must press and hold the “PTT” button to talk.

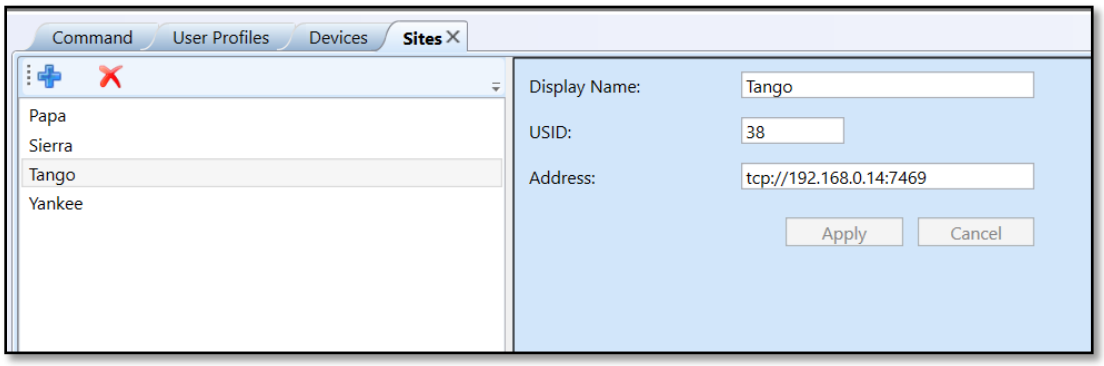
When the SIP device receives a call, an audible tone will be heard, and a ringing bell will be shown over the asset. To answer, long-press the ringing asset.

5.4 MultiSite and Site Editor

RADIUS MultiSite enables multiple RADIUS gateways to be federated across an IP network. In this configuration, operators connected to a local RADIUS gateway can, if permitted, monitor, patch, and control assets connected to remote RADIUS gateways.

The Site Editor allows the administrator to add, delete, or modify IP connections to RADIUS gateways participating in a MultiSite configuration.

In the example below, the Site Editor displays four configured sites. When a site is selected, its associated configuration details are shown in the panel on 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 via the gateway's front LCD panel.

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

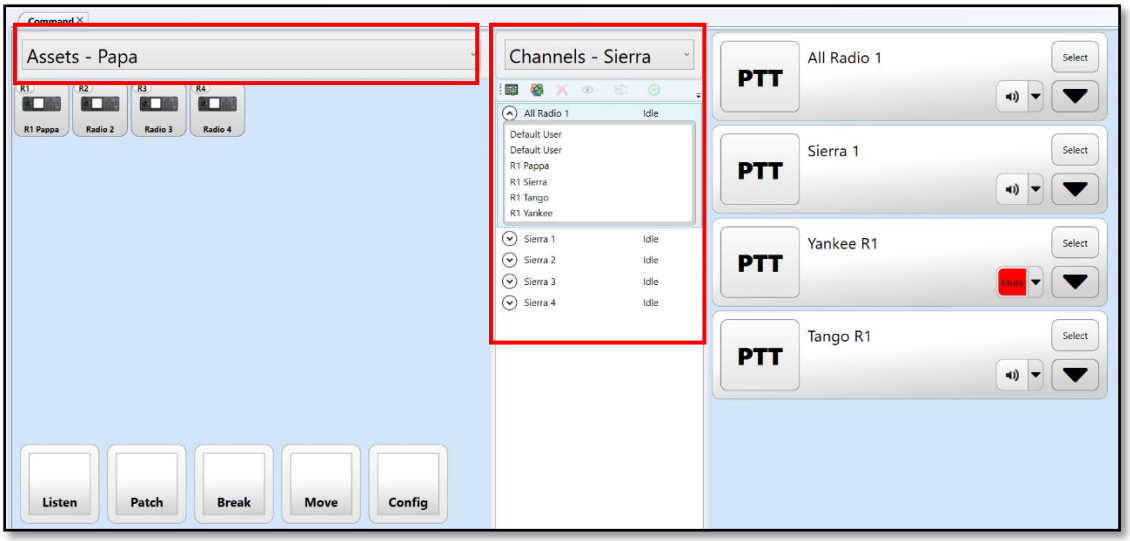
The image below shows the RADIUS GUI, which provides access to the RADIUS MultiSite configuration above. From the dropdown, the operator can choose the site to view or access the remote site's Assets. In the Channels Module, the dropdown allows the operator to view and select remote channels for their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

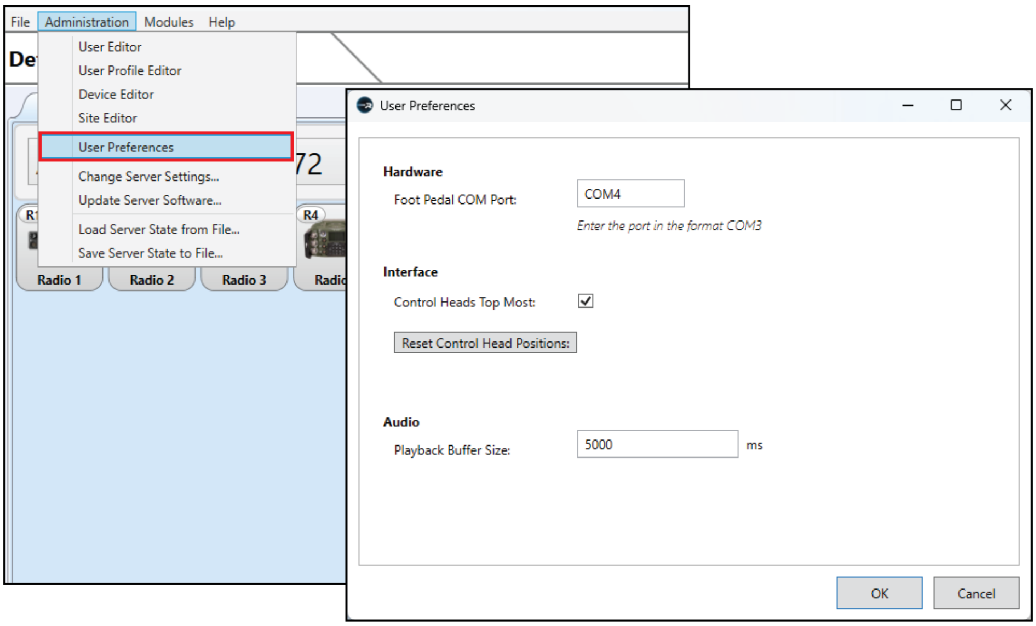
6. Repeat the process from the other gateway.

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



5.5 User Preferences

The User Preferences menu allows the operator to configure local client settings, including hardware interfaces, display behavior, and audio performance. To access User Preferences, select Administration from the menu bar, then choose User Preferences.



Hardware

- Foot Pedal COM Port – Specifies the COM port used for a connected foot pedal device. Enter the port in the format “COMX” (e.g., COM4). This setting enables push-to-talk (PTT) control via a foot pedal, if installed.

Interface

- Control Heads Top Most – When enabled, control head windows will remain on top of other application windows. This ensures visibility during operation.

- Reset Control Head Positions – Resets all control head window positions to their default layout. Use this option if control heads have been moved off-screen or require reorganization.

Audio

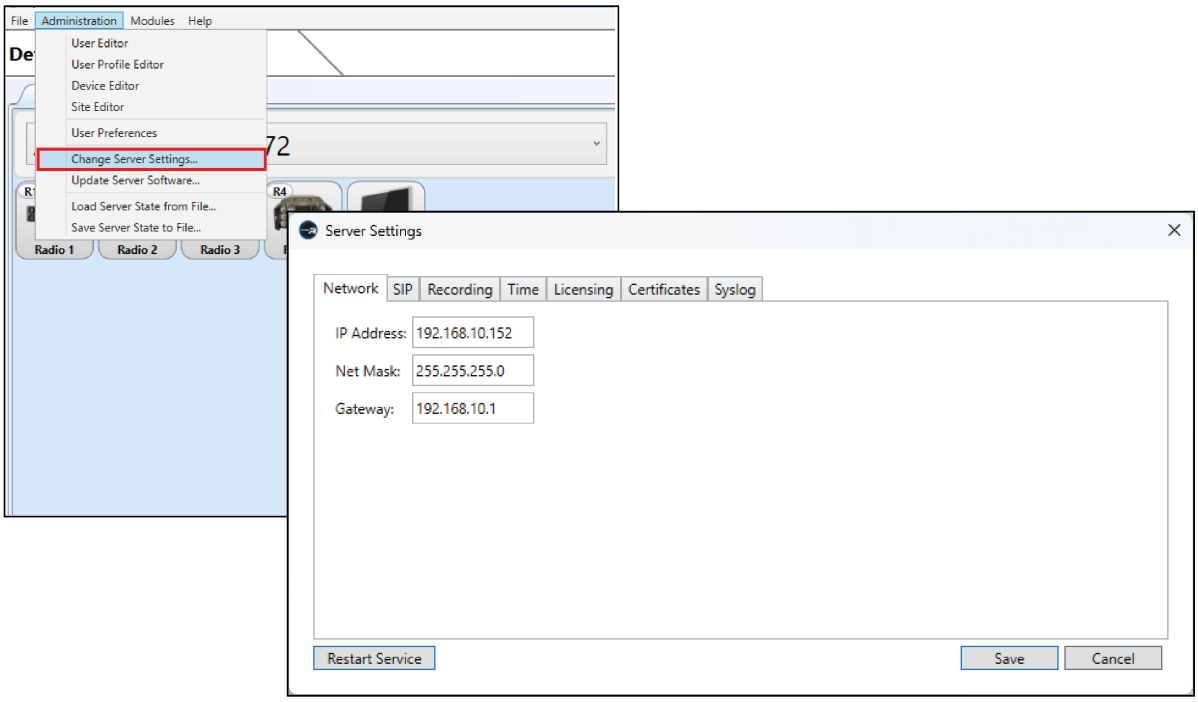
- Playback Buffer Size – Defines the audio playback buffer in milliseconds. Increasing the buffer size may improve audio stability on slower or congested networks but may introduce additional latency. Decreasing the buffer size reduces latency but may increase the risk of audio dropouts.

After configuring the desired settings, select OK. RADIUS Client will restart to apply the changes.

5.6 Change Server Settings

The **Change Server Settings** menu allows the administrator to configure system-level parameters for the RADIUS Distribution Service (DS), including network configuration, SIP integration, recording storage, system time, licensing, certificates, and logging.

To access Server Settings, select **Administration** from the menu bar, then select **Change Server Settings.**



The Server Settings window contains the following tabs:

5.6.1 Network

The **Network** tab allows the administrator to configure the IP settings of the RADIUS Distribution Service (DS).

The DS must be assigned an IP address that is valid for the target network and does not conflict with other devices. By default, the DS is configured with the IP address **192.168.0.10**.

To change the external IP address of the DS:

Log in to the RADIUS Client.
The client computer must be able to communicate with the current DS IP address.

From the menu bar, select **Administration, Change Server Settings.**

In the **Network** tab, enter the desired:

- IP Address
- Net Mask
- Gateway

Select **Save**, then restart the DS to apply the changes.

5.6.2 SIP Server Settings

The **SIP** tab enables integration with telephone systems using the Session Initiation Protocol (SIP).

- **Enabled** – Enables or disables SIP functionality.
- **SIP Server IP Address** – The IP address of the SIP server.
- **SIP Server Port** – The communication port used by the SIP server (default: 5060).
- **SIP Mode** – Selects the transport protocol (e.g., TCP).
- **Certificate File** – Loads a certificate for secure SIP communication.
- **DH File** – Loads Diffie-Hellman parameters for encryption.
- **Enable SIP Log** – Enables SIP logging for troubleshooting purposes.

SIP must be properly configured and licensed for telephone integration features to function.

5.6.3 Recording Configuration

The **Recording** tab configures the storage location for audio recordings.

- **Enabled** – Enables or disables recording functionality.
- **Server or NAS IP** – The IP address of the storage location.
- **File Share** – The shared folder used to store recordings.
- **User ID / Password** – Credentials required to access the file share.
- **Status** – Displays the current connection status to the storage location.
- **Reconnect** – Attempts to re-establish connection to the storage location.

The DS must have read/write access to the configured location. The RADIUS Client must have read access to retrieve and play back recordings.

5.6.4 Time

The **Time** tab configures the system clock used for timestamping recordings and events.

- **Use Time Server** – Enables synchronization with an external time server.
- **Time Server Address** – The IP address of the time server.
- **Sync Now** – Immediately synchronizes time with the configured server.
- **Current Server Time** – Displays the current system time of the DS.

• **Sync Server Time to Client Time** – Synchronizes the DS time with the local client computer.

Some RADIUS configurations include a built-in real-time clock (RTC). If a time server is unavailable, the system will remain operational; however, recording timestamps will default to 1979, and client logins will fail when using customer certificates due to incorrect system time.

5.6.5 Licensing

The **Licensing** tab displays system licensing information and available features.

- **Server Name / Organization** – Identifies the licensed system.
- **Options** – Lists enabled features (e.g., MultiSite, Recording, Radio Control).
- **Provisioned Device Profiles / Quantity** – Displays licensed device types and quantities.
- **Change License** – Allows the administrator to update the system license.

Licensing determines which modules and device profiles are available within the system.

5.6.6 Certificates Management

The **Certificates** tab manages system certificates used for secure communications.

- **Certificate List** – Displays installed certificates, including type, issued-to, and expiration date.
- **Add** – Adds a new certificate to the system.
- **Delete** – Removes a selected certificate.
- **Submit** – Applies certificate changes.

Certificates are used for secure communication, including TLS-based connections. For more information on this configuration, please contact SyTech for the “TLS Security Management” Addendum to this manual.

5.6.7 Syslog

The **Syslog** tab configures external logging for system events.

- **Enabled** – Enables or disables syslog functionality.
- **Syslog Service IP** – The IP address of the syslog server.
- **Syslog Service Port** – The port used for syslog communication (default: 514).
- **Protocol** – Selects the transport protocol (e.g., UDP).

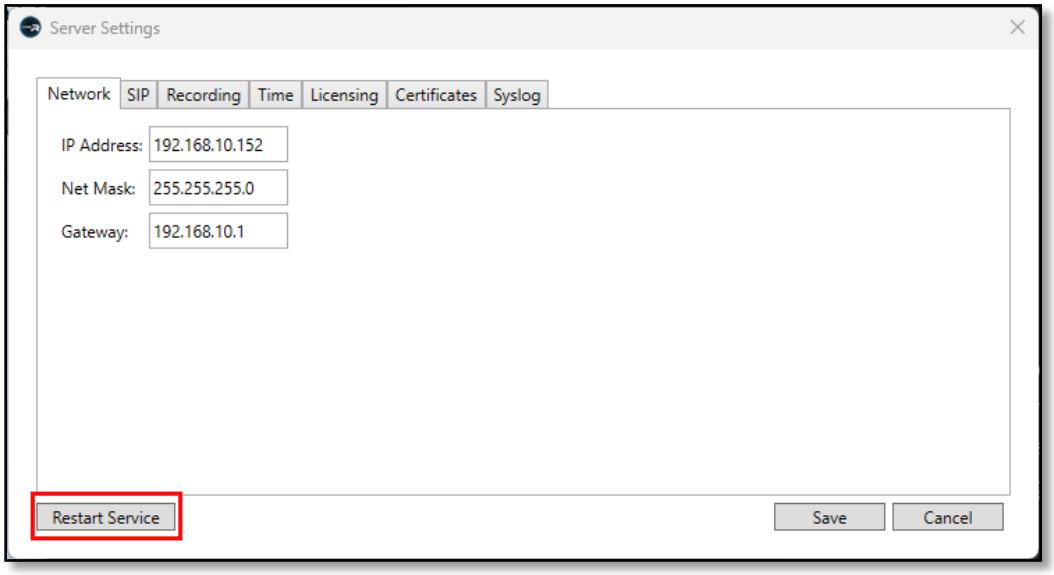
Syslog can be used for centralized logging, monitoring, and troubleshooting.

5.6.8 Saving and Applying the Changes

After configuring settings in any tab:

- Select **Save** to apply the changes.
- Select **Restart Service** to restart the DS if required.
- Select **Cancel** to exit without saving changes.

Some changes, such as network or service configurations, require a restart of the DS to take effect.



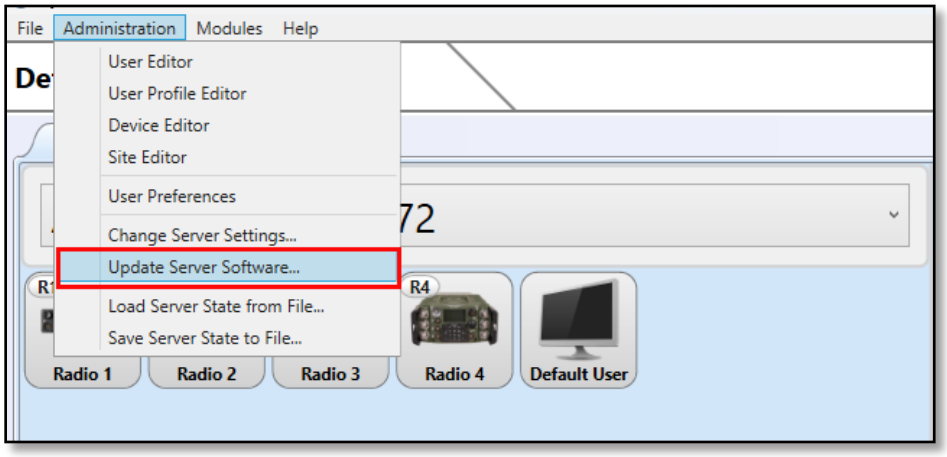
The operator can restart the DS remotely from within the RADIUS Client. Select Administration, Change Server Settings, and within the Network tab, select “Restart Service.”

5.7 Updating the RADIUS DS

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

To update the DS Software:

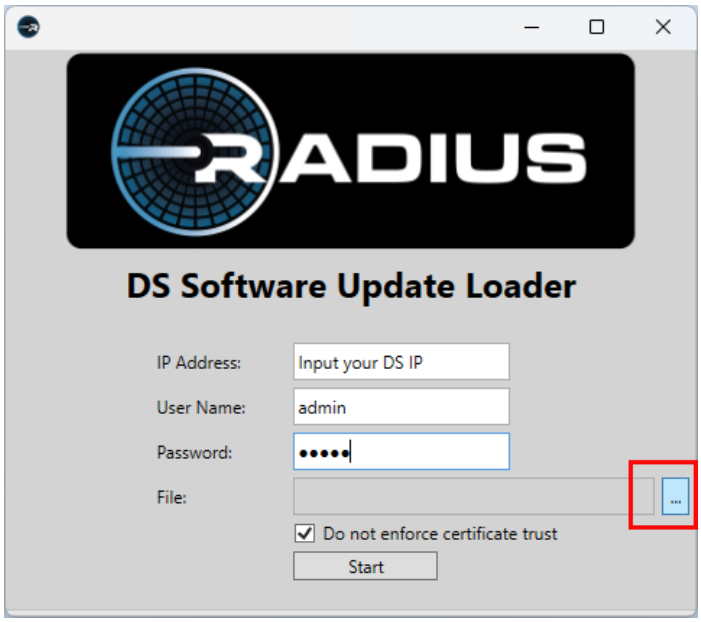
1. Select the “Update Server Software” from the Administration tab.



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.

2. 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 “XX.am62.RADIUSfw” to load the desired RADIUS DS firmware.



4. By default, a SyTech self-signed certificate is used. If customer certificates are not implemented, select “Do not enforce certificate trust.”

5. Select “Start.” The update tool will attempt to connect to the DS. If the connection is successful, the status will display “Connected.”

   If “Connected” is not displayed, there is an issue with the connection to the DS. Possible causes include network connectivity issues, an incorrect IP address, or invalid login credentials. Troubleshoot accordingly.

6. The updater will update the DS firmware and the RIB application on each RIB. Systems with a larger number of RIBs may require additional time to complete the update. During the update process, the blue LEDs will flash to indicate progress.

   When the update is complete, the DS Updater will automatically restart the DS. The process typically takes between five and ten minutes to complete.

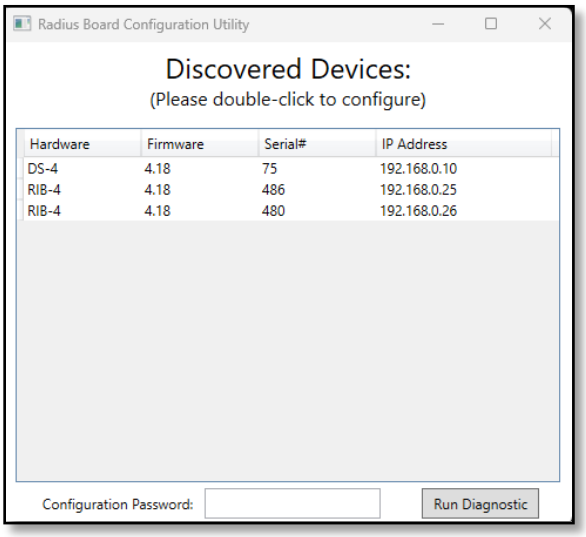
   If a RADIUS Client update is available, install it using the corresponding .msi file.

6. RADIUS BOARD CONFIGURATION UTILITY

The RADIUS Board Configuration Utility is a standalone application that allows advanced system administrators to scan for systems and configure IP settings for RADIUS devices, including nPoints and RADIUS DSs.

After installing the RADIUS Client, the RADIUS Board Configuration Utility is located in C:\Program Files (x86) \ SyTech. Double-click the application titled "RADIUS.Tools.BoardConfig.BoardConfigUtil."

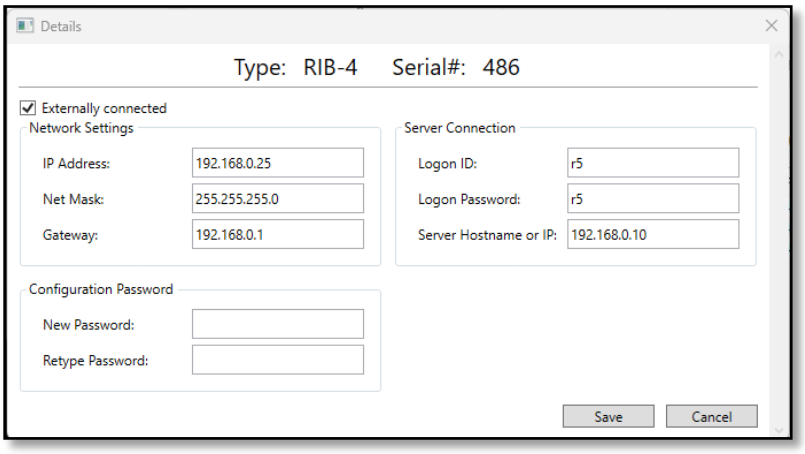
The utility will scan the network for available RADIUS servers. In the graphic below, the utility has located three devices: one DS (Distribution Server) and two RIBs (Radio Interface Boards). The firmware version, serial number, and IP address of the devices are displayed.



6.1 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 Settings, changing the necessary configurations as needed.

   The “Network Settings” refer to the device's settings. This includes the device's IP address, 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 in the Device Editor of 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 appear correctly in the DS.

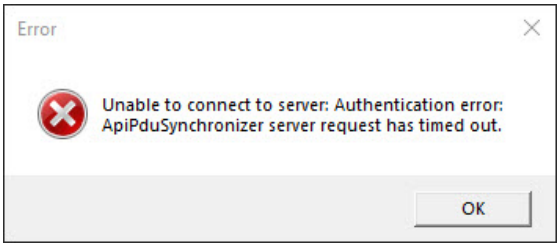
5. Select “Save.” The device will reset (if it does not, manually reset it).

7. 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 returns the error: “Unable to connect to Server: Authentication error: ApiPDUSychronizer server request timed out.”



Reason: The Client cannot locate the server.

Resolution. Confirm that the client computer can ping the server's IP address from the Command Line Prompt. If the server cannot be reached, verify that the network settings are compatible with the gateway (you may need to temporarily change your computer's IP address to match the gateway's IP settings). See Section 5.5 for instructions on changing the External DS IP Address.

Symptom: The IP address of the DS is unkown and there is no LCD screen.

Reason: Some RADIUS configurations, such as the PacStar 467 module, do not have LCD screens.

Resolution: Use the RADIUS Board Configuration utility as described in Section 7. The utility is a separate Microsoft application. Contact SyTech or your administrator if you do not have access to the utility.

AUDIO

Symptom: When a PTT is initially turned on, the channel does not transmit or turn green (indicating that audio is being received). When the PTT is released, the button flickers red.

Reason: RADIUS is requesting a microphone input, but no microphone is assigned.

Resolution. Connect a microphone, or indicate which microphone to use. You may need to restart the RADIUS client.