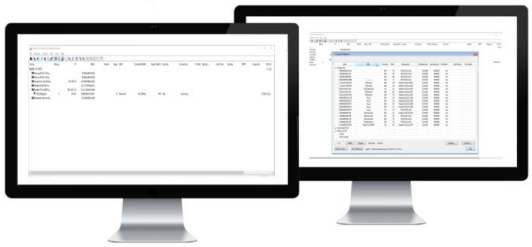
ProSoft TECHNOLOGY

Where Automation Connects.



IH Browser

PSW-RLX-IHB

Software Utility

May 2, 2025

USER MANUAL

Your Feedback Please

We always want you to feel that you made the right decision to use our products. If you have suggestions, comments, compliments or complaints about our products, documentation, or support, please write or call us.

ProSoft Technology, Inc.
+1 (661) 716-5100
+1 (661) 716-5101 (Fax)
www.prosoft-technology.com
ps.support@belden.com

IH Browser User Manual
For Public Use.

May 2, 2025

Content Disclaimer

This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither ProSoft Technology nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. Information in this document including illustrations, specifications and dimensions may contain technical inaccuracies or typographical errors. ProSoft Technology makes no warranty or representation as to its accuracy and assumes no liability for and reserves the right to correct such inaccuracies or errors at any time without notice. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying, without express written permission of ProSoft Technology. All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components. When devices are used for applications with technical safety requirements, the relevant instructions must be followed. Failure to use ProSoft Technology software or approved software with our hardware products may result in injury, harm, or improper operating results. Failure to observe this information can result in injury or equipment damage.

For professional users in the European Union
If you wish to discard electrical and electronic equipment (EEE), please contact your dealer or supplier for further information.

Prop 65 Warning – Cancer and Reproductive Harm – www.P65Warnings.ca.gov

Agency Approvals and Certifications

Please visit our website: www.prosoft-technology.com

Table of Contents

1 Installing the RadioLinx Industrial Hotspot Browser

Use the *RadioLinx Industrial Hotspot Browser* Configuration Tool (hereafter called the *IH Browser*) to set up and configure the RLX2/ELXM series radios. It is designed for personal computers running the Microsoft Windows operating systems.

1.1 IH Browser System Requirements

The IH Browser is designed to run on Microsoft Windows, and is supported on the following versions:

- Microsoft Windows 7 Professional 32- or 64-bit, with Service Pack 1
- Microsoft Windows 10
- Microsoft Windows 11

Other Microsoft Windows operating system versions may work but have not been tested by ProSoft Technology and are not officially supported.

1.2 Installing IH Browser Software

Install the RadioLinx Industrial Hotspot Browser (IH Browser) software to discover and connect to the radio as the RLX2/ELXM series radios are not shipped with a default static IP Address.

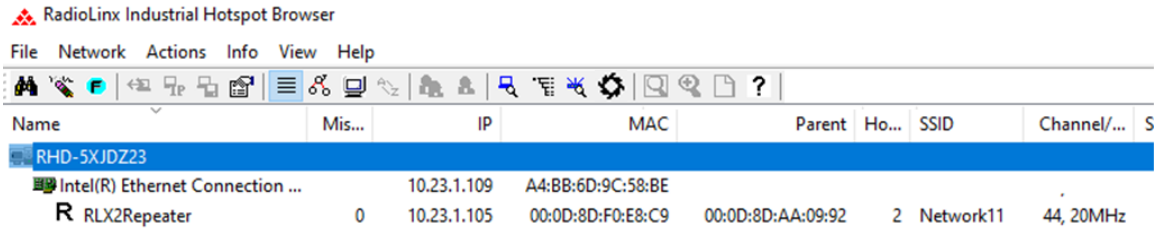
1. Open your web browser and navigate to www.prosoft-technology.com
2. Use the search box on the ProSoft Technology page to search for "**IH Browser**" and then click the link for the *RadioLinx IH Browser*.
3. Click the *Download* tab and then click **RADIOLINX IH BROWSER** to download the latest version of the IH Browser.
4. Choose **SAVE** or **SAVE FILE** when prompted.
5. Save the file to your Windows Desktop.
6. When the download is complete, locate and double-click the zip file to extract the installation file (RadioLinx IH Browser 3.130.msi or a newer version).
7. Double-click the **.msi** file to install the IH Browser.

If your computer does not have access to the Internet, you must download the software from the ProSoft Technology website to removable media, and then copy it to your computer.

2 Using the IH Browser to Manage your Radios

Start the IH Brower. If the RLX2/ELXM series radio is powered up and connected, it appears in the IH Browser. Note that the *MAC* address is the same address as that of the label on the radio.

The *List* view displays the radios on the same network as the computer running the IH Browser.



Note: You can perform many common tasks by right-clicking on the radio and choosing a command.

2.1 Refreshing the Display in the IH Browser

If the radio's configuration has been changed, refresh the IH Browser by clearing and scanning the display using the buttons on the toolbar.

The *Erase* button clears the radios from display (or from the **FILE** menu choose **CLEAR**).

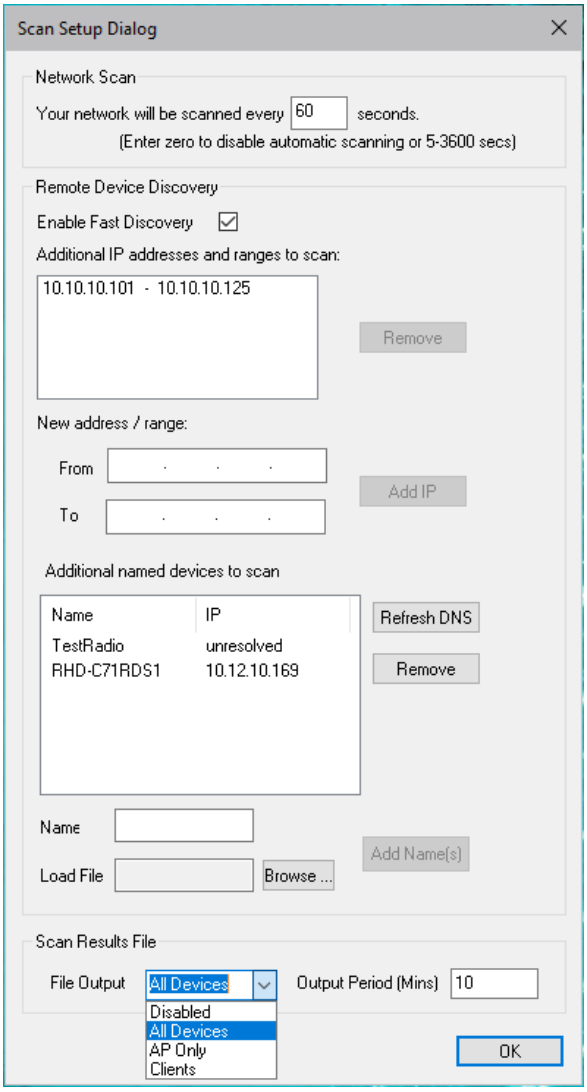
The *Scan* button rescans the network for RLX2/ELXM series radios (or from the **FILE** menu choose **SCAN**).

2.2 Defining the Scan Parameters in the IH Browser

Use the *Scan Setup* dialog box to specify how the IH Browser refreshes the display when scanning the network. By default, the program sends a broadcast Scan message to all the radios at the same time, then waits for them to respond. Broadcasts are limited to a local network, and will not be passed through a router.

If there is a router between the PC running the IH Browser and the radio, enter the IP address of a single radio or the range of IP addresses of multiple radios. This adds them to the IP addresses the IH Browser scans.

To define the scan parameters, from the **NETWORK** menu, choose **SCAN SETUP**.



Parameter	Description
Network Scan	
Local network scanning interval	Specifies how often the IH Browser scans the network and updates the display. Enter **0** to disable automatic scanning. You can still scan the network manually.
Remote Device Discovery	Parameters related to communicating to radios that are on a different subnet than the PC running the IH Browser.
Enable Fast Discovery	The additional addresses or names will be discovered in the background. By selecting this option, the discovery will proceed at a faster rate at the expense of network traffic.
Additional IP addresses	Displays the IP addresses the IH Browser scans at the scanning interval.
Remove	Removes the selected IP address or range. Click on an IP address or address range to select it.
New Address / Range	Enter the new IP address (in **FROM**) or range of IP addresses (in **FROM** and **TO**) and then click **ADD IP** button.
Additional Named Devices	Displays the Device Names to scan. (Requires that the name of the RLX2 or ELXM radio has been registered with a DNS server.)
Name	Adds a new name to the list.
Load File	Adds a list of names from a text file.
Refresh DNS	Updates the results of a DNS query on each name.
Remove	Removes the selected name from the list.
Add Name(s)	Adds the individual name or list of names to the list. A DNS query will be completed for each name.
Scan Results File	Parameters related to writing status of radios discovered by the IH Browser to a json formatted output_log.json file in a Windows hidden folder. To locate the file, enter C:\ProgramData\Prosoft\ in the Windows File Explorer Address Bar.
File Output	Select box with options to: **Disable**: Disable outputting to the file. **All Devices**: Output data on all discovered radios. **AP Only**: Output data only on discovered Access Points. **Clients**: Output data only on discovered Client radios.
Output Period	The interval in minutes which the json formatted file is overwritten with the current snapshot of information on radios known to the IH Browser.

2.3 Freezing the Display in the IH Browser

Freezing the display in the IH Browser prevents it from updating with new data.

The *Freeze* button on the IH Browser toolbar prevents the display from updating (or from the **FILE** menu choose **FREEZE**).

Click the *Freeze* button again to start updating the display.

2.4 Changing IH Browser Columns in List View

You can change the columns that appear in the IH Browser main window in *List View*.

1 From the **VIEW** menu, click **SELECT COLUMNS**.

2 In the *Select Columns* dialog box, click the check boxes for the columns you want to appear in the window.

To reset the columns in the IH Browser window to the default, from the **VIEW** menu, click **RESET COLUMNS**.

2.5 Switching between List and Topology Views

You can switch between the List and Topology Views in the IH Browser main window.

- The *List View* is the default view, and shows a list of all the connected radios in a grid, similar to a spreadsheet.
- The *Topology View* shows a diagram of the network's wireless connections. If a radio does not appear in the view, it is not connected to the network. The Topology View is display-only.

To switch between the List and Topology views

- The *List View* button switches to the List View (or from the **VIEW** menu choose **LIST VIEW**). For a description of the available columns, see section *2.5.1 List View Columns*.
- The *Topology View* button switches to the Topology View (or from the **VIEW** menu choose **TOPOLOGY VIEW**). For a description of the *Topology View*, see section *2.5.2 Topology View Description*.

To change the columns in the List View

- To resize a column, click between column headers and drag left or right.
- To re-order the columns, click a column header and drag it to the left or right.
- To sort the radios, click a column header to change the sort order
- To change the displayed columns, from the **VIEW** menu choose **SELECT COLUMNS**.

To zoom in and out in the Topology View

- The *Zoom In* button magnifies the *Topology View* (or from the **VIEW** menu choose **ZOOM IN**).
- The *Zoom Out* button shrinks the *Topology View* (or from the **VIEW** menu choose **ZOOM OUT**).
- The *Zoom to Fit* button resizes the *Topology View* to fit the window (or from the **VIEW** menu choose **ZOOM TO FIT**).

To sort radios alphabetically in the Topology View

- The *Sort Alphabetically* button sorts the radios in the by name *Topology View* (or from the **VIEW** menu choose **SORT ALPHABETICALLY**).

To change a radio's configuration in either view

Double-click a radio to launch a web browser to the login page of the radio. See Chapter *6 Connecting to the Radio Configuration Interface*.

2.5.1 List View Columns

This topic describes the available columns in the *List View*. See section *2.5 Switching between List and Topology Views* for more information on the *List View* columns.

Note: You can display most of the same information for the radio in the *Detailed Information* dialog box the IH Browser. For more information, see chapter *3 Viewing the Radio Properties*.

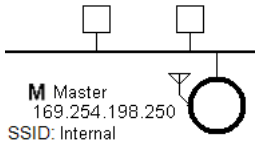
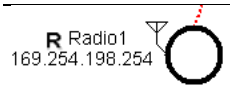
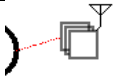
Column Name	Description
Name	Displays the radios in the IH Browser. Names appear in a nested tree order. The icons on some entries help identify the type of radio.  Computer  Network Interface  Master Radio  Repeater Radio  Ethernet Bridge Radio  Client Radio  Bridging Client Radio  Un-commissioned Radio
Mode	Displays a text description of the radios in the IH Browser. **THIS UTILITY**: This instance of the IH Browser. **UTILITY**: Other instances of IH Browsers running on other systems on the same network. **LOCAL INTERFACE**: A network interface detected on the computer running this instance of the IH Browser. **MASTER**: A radio on the network in Master mode. **CLIENT**: A radio on the network in Client mode. **BRIDGING CLIENT**: A radio on the network in Bridging Client mode. **ETHERNET BRIDGE**: A radio on the network in Ethernet Bridge mode. **REPEATER**: A radio in the network in Repeater mode.
MAC	Displays the physical Media Access Control (MAC) address of the radios. All ProSoft Technology radios have a MAC address in the form 00:0D:8D:XX:YY:ZZ.
IP	Displays the IP addresses assigned to the radios.
Mask	Displays the network mask for the radio.
Gateway	Displays the IP address of the network gateway for the radio.

SSID	Displays the Service Set Identifier (SSID). This is a name assigned to a wireless network radio. Repeater and Client radios must be configured with the same SSID to connect. Note that Master radios typically broadcast their SSID. However, you can disable SSID broadcasting so that other wireless radios cannot detect the Master radio. If a Master is not broadcasting its SSID, this field includes the word **HIDDEN** along with the SSID of the radio; for example, *ProSoft/hidden*.
Connection	Displays the connection state for a Repeater radio. **SCANNING**: The radio is searching for a Master radio. **CONNECTED**: The radio is linked to a Master radio.
Signal (dBm)	Displays the signal strength in dBm of a Repeater or Client radio's link to a Master radio. Master radios do not report signal strength.
Hops	Displays the number of wireless connections from the radio to the wired connection of a Master. This value is always **1** for a Master radio. For Repeater radios, the value is at least **2** but can be higher if there are more hops to the Master radio. Client radios do not display a hop value.
Parent	Displays the MAC address of the Parent radio to which this Repeater or Client radio is linked. This is blank for Master radios.
Associations	Displays the number of non-bridge wireless connections to this radio. Client or Bridging Client radios that are connected always show **1** in this column (and **0** in the *Bridges* column).
Bridges	Displays the number of non-bridge wireless connections to this radio. Client or Bridging Client radios that are connected always show **1** in this column (and **0** in the *Bridges* column).
Tx (kbits/sec)	Displays a moving average of transmit throughput in kilobits/second. It does not count packet overhead, and only counts payload data. For Repeater radios, this shows the throughput only for the radio link to the Parent radio. For Master radios, this is the throughput sum of all the Master's radio links.
Rx (kbits/sec)	Displays a moving average of receive throughput in kilobits/second. It does not count packet overhead, and only counts payload data. For Repeater radios, this shows the throughput only for the radio link to the Parent radio. For Master radios, this is the throughput sum of all the Master's radio links.
FW Ver	Displays the firmware version number. For IH Browser entries, this is the version of the IH Browser itself. For radios, this is the version of the firmware code in the radio. This is not the version of the image file installed into the radio (for that information see **IMAGE VER** described below).
Boot Ver	Displays the boot loader code version number. For IH Browser entries, this is the version of the network communication engine in the IH Browser (e.g. WinXP, WinVista). For radios, this is the version of the boot loader code in the radio.
Image	Displays the type of the firmware image that the radio is currently running (**PRIMARY** or **SECONDARY**). Each radio has two copies of operating firmware installed, and the radio will automatically switch from one to the other if one of them becomes corrupted.
Compression	Displays the compression state of the firmware images in the radio (**COMPRESSED** or **UNCOMPRESSED**).
Ethernet	Displays the Ethernet status for the radio. **ATTACHED:** The radio is connected to a wired Ethernet network. **DETACHED:** The radio is not connected to a wired Ethernet network.
Channel/Width	Displays the operating channel and channel width. The width value can be 20MHz, 40MHz or 80MHz. Example: **48, 20 MHz** for channel 48 with a 20 MHz channel width.
Security	Displays the encryption type setting for the radio. Some valid settings are **AES**, **TKIP**, **AES&TKIP**, **WEP128 TKIP**, **WEP128**, **WEP64**.
Misses	Displays the number of times the IH Browser has failed to receive a response from the radio after a scan. Ideally this number should always be **0**.

RSTP	Displays the setting for RSTP in the radio (**ENABLED**, **DISABLED**, and **STP**). The STP state is a legacy "non-rapid" Spanning Tree mode that the radio automatically uses if it detects a peer wired bridge in STP mode. All radios on a network must have the same RSTP state to link properly.
Link Time	Displays the link time of the radio. For example, **24d,13h,10m,32s**. This time resets to **0** on a Roam, or if the link is dropped and re-established with the same Parent radio.
Tx Rate	Displays the current modulation data rate that the radio is using for transmission. This may be slower than the configured nominal rate because of retries or other environmental factors. For 802.11a/b/g radios, the data rate is expressed in kilobits or megabits per second (for example, **54Mb/s**). For 802.11n/ac/ax radios, the data is expressed in MCS rates from 0 to 15 (for example, **MCS7**).
Retries(%)	Displays the ratio of packet re-transmission to total packet transmissions during the last five-second interval for the radio.
Uptime	Displays the amount of time the radio has been running since the last power cycle or reset; for example, **1d,4h,13m,25s**.
Product	Displays the model number of the RLX2 radio; for example, **RLX2-IHA**, **RLX2-IHG**, **RLX2-IHFN**, **RLX2-IHFN-W**, or **RLX2-IHW**.
Image Ver	Displays the name of the image file loaded into the radio; for example, **RLX2_v0036_R**.
Tx Pkts/Sec	Displays a moving average of transmitted data packets/second. For Repeater radios, this shows the data packet rate transmitted over the radio link to the Parent radio. For Master radios, this is the transmitted data packet rate sum on all the Master's radio links.
Rx Pkts/Sec	Displays a moving average of received data packets/second. For Repeater radios, this shows the data packet rate received over the radio link to the Parent radio. For Master radios, this is the received data packet rate sum on all the Master's radio links.

2.5.2 Topology View Description

This topic describes the *Topology View*. See section *2.5 Switching between List and Topology Views* for more information on the *Topology View*.

Topology View	Description
	Indicates the Master radio; always shown at the top.
	Indicates a radio linked to the network.
	Indicates a radio not linked to a Parent radio, but on the same network as the computer hosting the IH Browser.
	Indicates that an Ethernet connection exists to the radio but does not indicate the number of radios on the connection.
	Indicates that wireless clients (such as laptops and tablet computers) are linked to this radio. The number of clients linked is indicated by the number of boxes and/or a number.
	Indicates signal strength between radios. The width of the line is not calibrated, but a wider line indicates a relatively stronger signal strength.
	Indicates links to alternate Parent radio candidates that could be chosen if the current Parent link drops or degrades.

2.6 Printing the View in the IH Browser

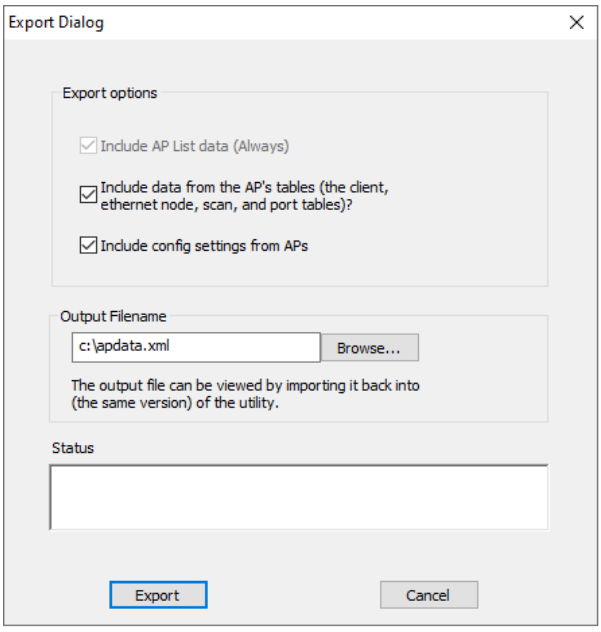
You can print the current view in the IH Browser.

- To print the current view, from the **FILE** menu choose **PRINT**.
- To define the page orientation, paper source, and size, from the **FILE** menu choose **PRINT SETUP**.
- To preview the printed view, from the **FILE** menu choose **PRINT PREVIEW**. This can help you adjust the view in the IH Browser so it does not break across pages when printed.
- In the *Topology View*, to display a border around the area to be printed, do one of the following:
  - From the **VIEW** menu, choose **PRINT AREA**.
  - On the IH Browser toolbar click the *Show Page Outline* button.

2.7 Importing and Exporting IH Browser Data

You can export data from, and import data into, the IH Browser. Exporting data creates and saves an XML file containing the current configuration and status of all radios discovered by the IH Browser. You can use this command under the direction of ProSoft Technical Support, for troubleshooting purposes. Importing data brings in the data from a previously created IH Browser XML file.

- To export data from the IH Browser, from the **FILE** menu choose **EXPORT**. You can choose to include the data from the current *Wireless Client*, *Ethernet Nodes*, *Scan List*, and *Port Table* tables. See chapter *5 Viewing Additional Data in the IH Browser* for more information.

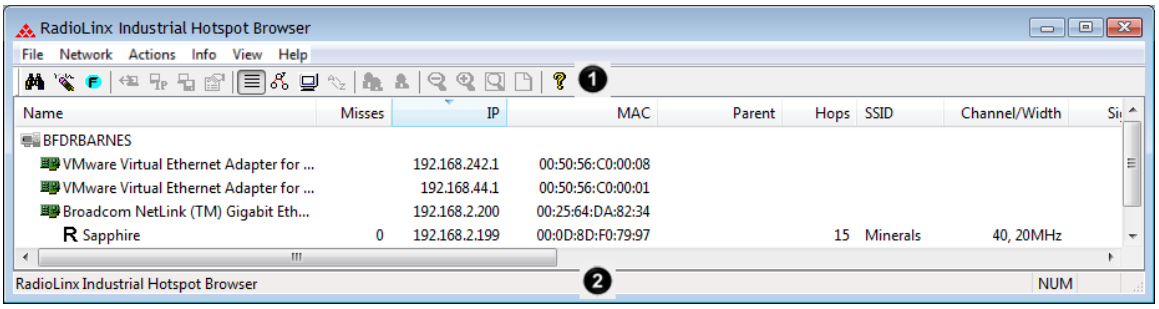


- To import data from an export file created in the IH Browser, from the **FILE** menu choose **IMPORT**.

2.8 Hiding the Toolbar and Status Bar in the IH Browser

You can hide and display the Toolbar and Status bar in the IH Browser window.

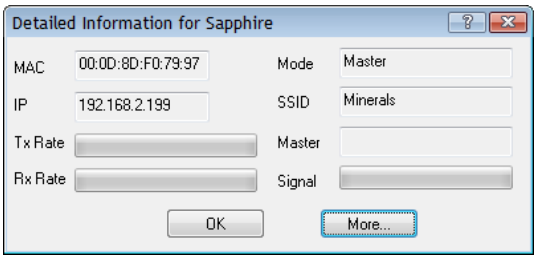
- To hide and show the Toolbar (**1** in the image below), from the **VIEW** menu choose **TOOLBAR**.
- To hide and show the Status Bar (**2** in the image below), from the **VIEW** menu choose **STATUS BAR**.



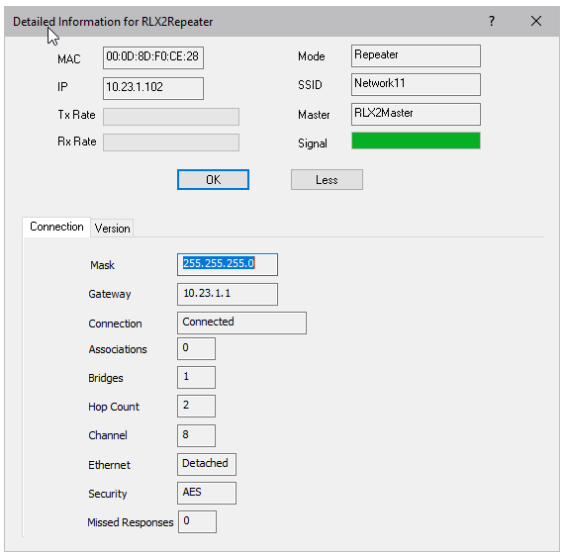
3 Viewing the Radio Properties

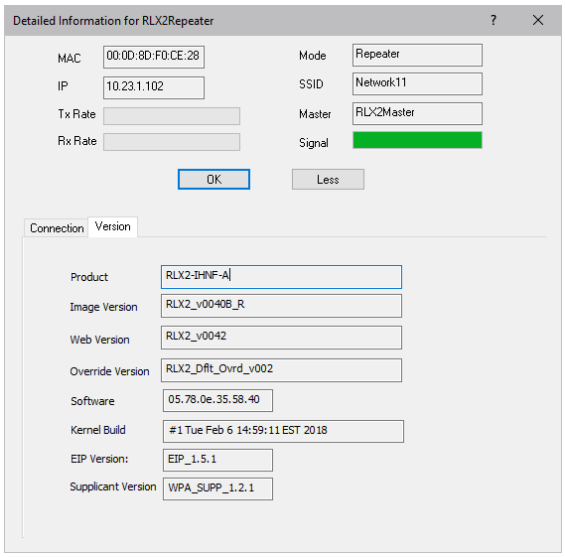
The *Detailed Information* dialog box shows information about the currently selected radio.

1. In the IH Browser, select (click) a radio in either the *List View* or *Topology View*.
2. From the **INFO** menu choose **PROPERTIES**, or right-click the radio and choose **PROPERTIES**.



3. Click **MORE** to display more information.





Note: You can display most of the same information in the *List View* in the IH Browser. For more information, see section *2.5.1 List View Columns*.

Parameter	Description
MAC	Displays the MAC address of the selected radio.
IP	Displays the IP address of the selected radio.
Mode	Displays the mode of the selected radio (**MASTER**, **REPEATER**, **BRIDGE**, **CLIENT**, **BRIDGING CLIENT**)
SSID	Displays the SSID of the selected radio.
TX Rate	Displays a green bar when there is transmit activity.
RX Rate	Displays a green bar when there is receive activity.
Master	Displays the MAC address of the radio's current Master radio.

Parameter	Description
Signal	Displays a green bar when there is a signal.
More / Less	Click **MORE** to expand the dialog box and display more information. Click **LESS** to reduce the dialog box and display less information.
Connection / Version tabs	Tabs showing information related to the radio's connection and the version of the radio's various components.
Connection	
Mask	Displays the network mask for the current radio.
Gateway	Displays the network gateway IP for the current radio.
Connection	Displays the connection state for a Repeater radio. **SCANNING** - The radio is searching for a Master radio. **CONNECTED** - The radio is linked to a Master radio.
Associations	Displays the number of non-bridge wireless connections to this radio. Client or Bridging Client radios that are connected always show 1 in this column (and 0 in the Bridges column).
Bridges	Displays the number of non-bridge wireless connections to this radio. Client or Bridging Client radios that are connected always show 1 in this column (and 0 in the Bridges column).
Hop Count	Displays the number of wireless connections from the radio to the wired connection of a Master. This value is always 1 for a Master radio. For Repeater radios, the value is at least 2 but can be higher if there are more hops to the Master radio. Client radio does not display a hop value.
Channel	Displays the operating channel for radio.
Ethernet	Displays the Ethernet status for the radio. **ATTACHED** - The radio is connected to a wired Ethernet network. **DETACHED** - The radio is not connected to a wired Ethernet network.
Security	Displays the encryption type setting for the radio. Some valid settings are **AES**, **TKIP**, **AES&TKIP**, **WEP128 TKIP**, **WEP128**, **WEP64**.
Missed Responses	Displays the number of times the IH Browser has failed to receive a response from the radio after a scan. Ideally this number should always be zero.
Version	
Product	Displays the radio's Model Name.
Image Version	Displays the software Image File version that the radio is currently running.
Web Version	Displays the version of the set of web pages used by the radio's web server.
Override Version	Displays the version of a file containing factory defaults that differ from built-in values.
Software	Displays the version of the firmware wireless code in the radio. This is not the *Image Version* of the image file installed into the radio.
Kernel Build	Displays the build time of the Kernel running in the radio
EIP Version	Displays the version of the EtherNet/IP agent running in the radio.
Supplicant Version	Displays the version of the WPA Supplicant running in the radio.

4 Setting the Radio IP Address in the IH Browser

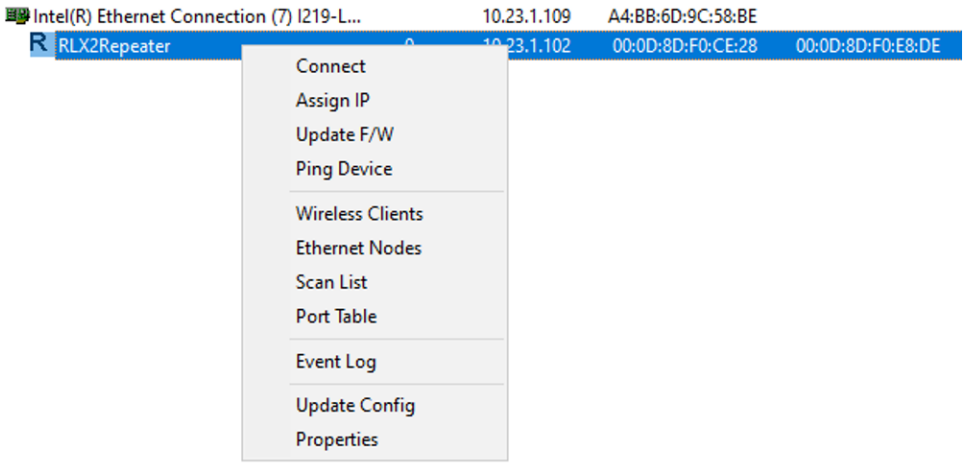
If the radio is on a network with a DHCP server, it gets an IP address through DHCP.

If the radio is not on a network with a DHCP server, the radio appears with an IP address of **0.0.0.0**. Assign a temporary IP address to assist with configuring the radio. For more information, see section *4.1 Assigning a Temporary IP Address*.

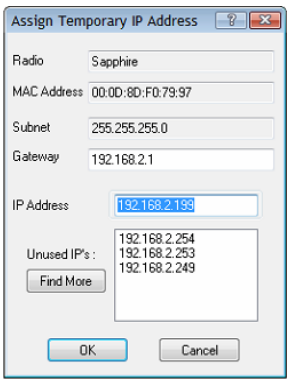
4.1 Assigning a Temporary IP Address

A temporary IP address allows you to access and configure a radio when the radio either does not have an IP Address or it has an IP Address that is on a network subnet different than the PC running the IH Browser.

1 In the IH Browser, right-click the radio and then click **ASSIGN IP**.

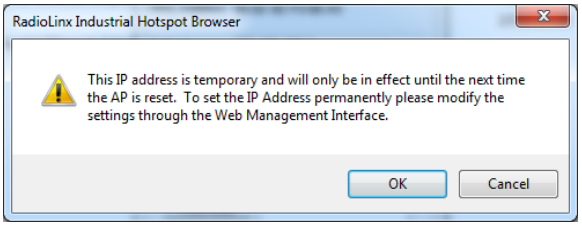


2 This opens the *Assign Temporary IP Address* dialog.



3 The **UNUSED IP'S** list are the IP addresses that are currently available on the network.

4 The IH Browser suggests the network parameters for the temporary IP address. It queries the IP addresses and displays them if it does not receive a response. Click one of the unused IPs, or enter an unused IP address, and click **OK**. The IH Browser warns you that the IP address is temporary.



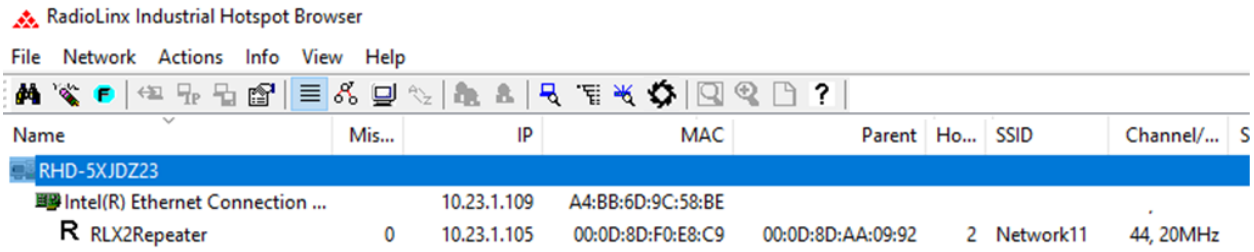
5 Click **OK** and refresh the display in the IH Browser. The radio should now appear in the IH Browser window with the temporary IP address.

6 To set a permanent IP address for the radio, see *Configuring a Radio - Getting Started* in the *RLX2 User Manual*. It can be downloaded at www.prosoft-technology.com.

5 Viewing Additional Data in the IH Browser

Start the IH Brower. If the radio is powered up and connected, it appears in the IH Browser. Note that the *MAC* address is the same address as that of the label on the radio.

The *List* view displays the RLX2/ELXM series radios (or previous generation RLXIB radios, except the RLCIB-IHN) on the same network as the computer running the IH Browser.



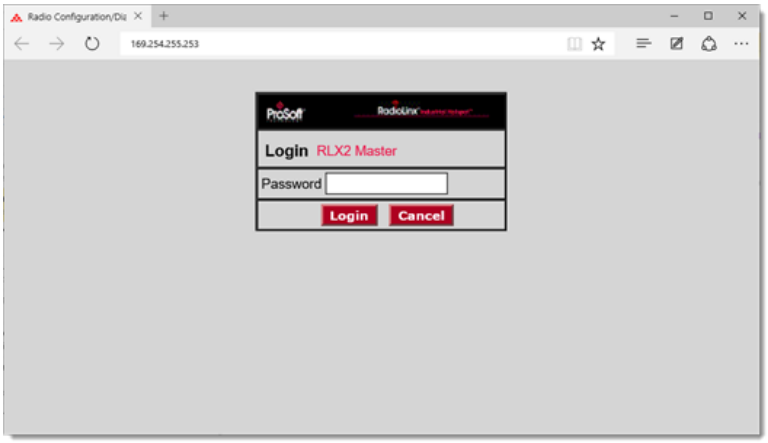
Note: You can perform many common tasks by right-clicking on the radio and choosing a command.

6 Connecting to the Radio Configuration Interface

This section describes how to configure a radio using a web browser such as Internet Explorer or Firefox on your PC or other network-enabled device.

Important: Your computer or other device must be connected to the same network as the RLX2/ELXM series radio.

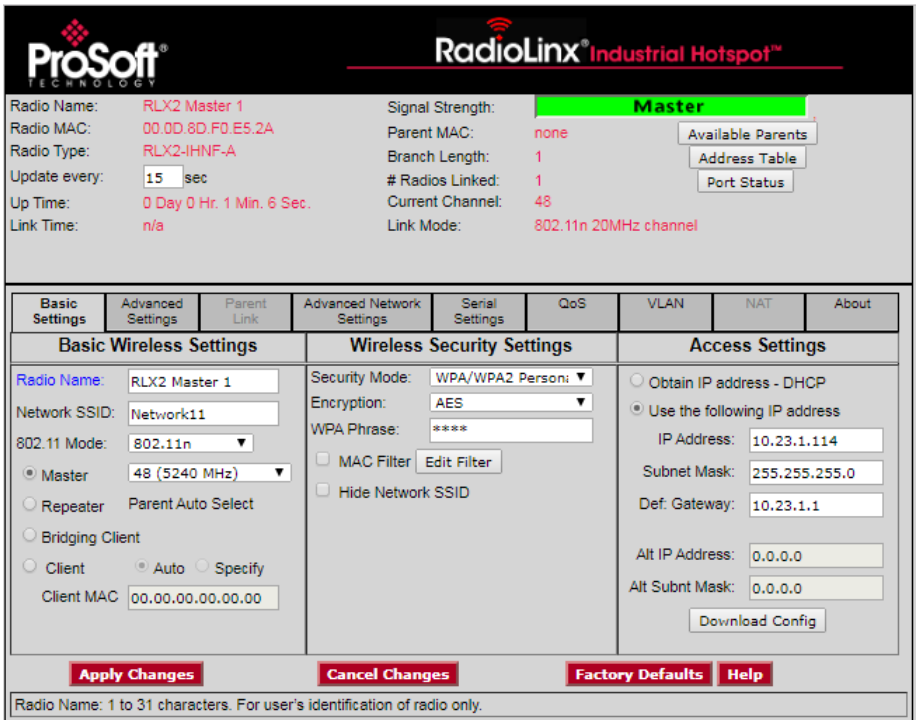
1. Log into the radio. You can do this in any of three ways:
   - In the IH Browser *List* view or *Topography* view, right-click the radio and then click **CONNECT**.
   - In the IH Browser *List* view or *Topography* view, double-click the radio.
   - Open a web browser on your PC, and then in the address bar, enter **`http://`**, followed by the IP address for the radio, and then press **ENTER**. For example, **`http://192.168.6.10`**.
2. The login screen appears in the web browser.



3. Enter the password and then click **LOGIN**. The default password is *password*.

Note: If the radio is using its factory defaults you will need to enter a new password before you can proceed to make changes to the settings.

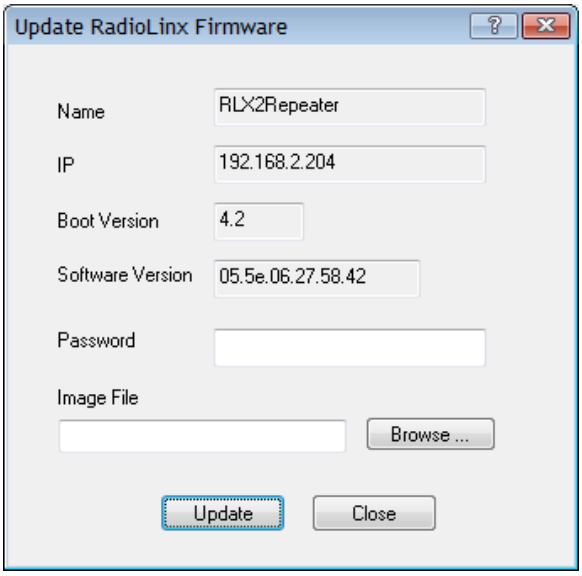
4. If you have lost the password for the radio, you can reset the radio to its default settings. See *Resetting a RLX2/ELXM Series Radio* in the *RLX2 User Manual*. It can be downloaded at www.prosoft-technology.com.
5. This opens the main webpage for the radio. Note that some parameters may be different from the following image depending on your specific radio model.



Tip: You can display the help topic for any parameter by clicking the parameter name. The parameter name turns blue when you move the cursor over a parameter with a help topic. There is also a short description of the cursor control at the bottom of the window.

7 Updating the Radio Firmware

ProSoft Technology may release new firmware for the RLX2/ELXM series radio that may include new features and corrected anomalies. We recommend that all RLX2/ELXM series radios in a network use the same firmware version. If your network has a mix of RLX2/ELXM series models, you can load the same firmware image file into each of them.



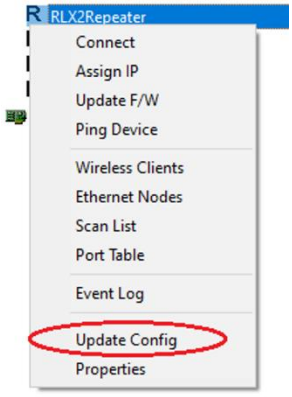
1. Download the radio firmware image from www.prosoft-technology.com and save it to a known location (such as the Windows Desktop).
2. Start the IH Browser and click on an RLX2/ELXM series radio to select it.
3. From the **ACTIONS** menu choose **UPDATE FIRMWARE**. You can also right-click the radio and choose **UPDATE F/W**.
4. Enter the password for the radio. This is the same password that you use to log into the radio web interface.
5. Click **BROWSE** to locate the firmware image file to load.
6. Click **UPDATE** to begin copying the new firmware to the radio.

Important: Do not turn off power to the radio during this operation.

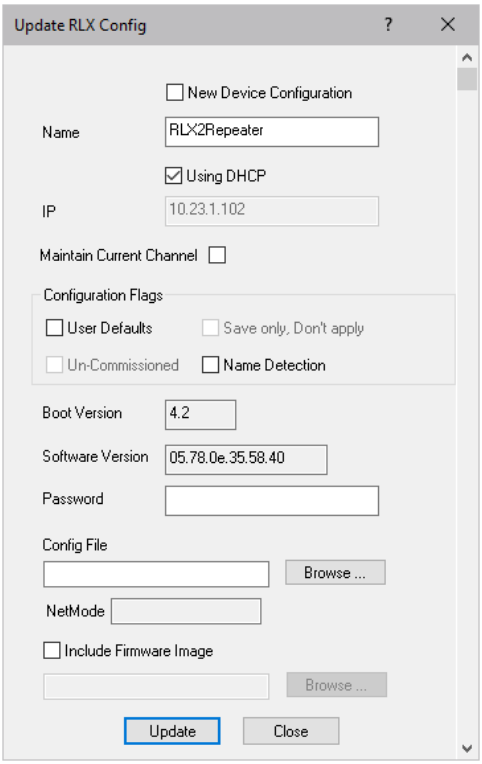
7.1 Updating the Radio's Configuration

This feature allows a user to configure the settings of an RLX2/ELXM series radio from a saved configuration file. The user would need to save the settings from an existing unit. This can be done through the radio's webpage.

1. Save the configuration file of an RLX2/ELXM series radio via its web interface to a known location (such as the Windows Desktop).
2. Start the IH Browser and click on an RLX2/ELXM series radio to select it.
3. From the **ACTIONS** menu choose **UPDATE CONFIG**. You can also right-click the radio and choose **UPDATE CONFIG**.



4. In the *Update RLX Config* dialog, enter the following parameters.



Parameter	Description
New Device Configuration	If this checkbox is selected all the parameters in this dialog will be remembered for the next radio that is to be configured.
Name	The name to be assigned to this radio.
Using DHCP	Select this checkbox if radio will use DHCP.
IP address	IP address to assign to this radio.
Maintain Current Channel	(Masters only) If this checkbox is selected the currently configured channel will be maintained overriding the channel specified in the configuration file.
Configuration Flags	These flags save configuration options in addition to those in the configuration file. **USER DEFAULTS**: This will save the configuration file to the radio as the User defined Defaults. **SAVE ONLY; DON'T APPLY**: This checkbox is enabled when the **USER DEFAULTS** checkbox is checked. When checked it will save the configuration file as the user defaults but will preserve the current configuration as the operating configuration. **UN-COMMISSIONED**: This checkbox is enabled when the **USER DEFAULTS** checkbox is checked. The un-commissioned parameter in the configuration will set to true. When the radio is reset to User Defaults it will then advertise itself as un-commissioned. **NAME DETECTION**: (Clients Only) When checked will add the *Learn name number* flag to the configuration. When the radio adopts this configuration, it will inspect DHCP Requests from Ethernet devices attached to this radio and extract any trailing number and append that number to the *Name* parameter in the configuration.
Boot Version	The current version of Boot code in the radio that is being updated.
Software Version	The current version of Software running in the radio that is being updated.
Password	The password for this radio.
Config File	The name/location of the configuration file.
NetMode	This will display the Network Mode (Master/Client) of the selected configuration file.
Include F/W image	Select this checkbox if you would also like to update the firmware of the radio.
Firmware file	The name/location of the firmware file.

5 Click **UPDATE** to begin copying the new configuration to the radio.

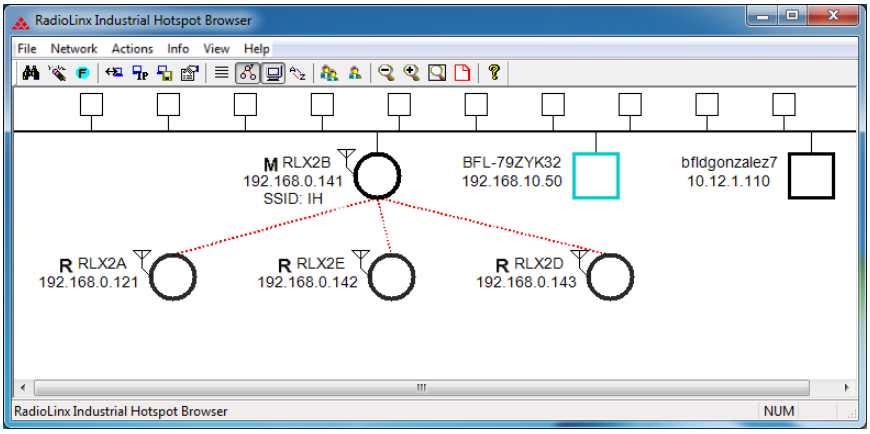
Important: Do not turn off power to the radio during this operation.

8 Pinging Radios on the Network

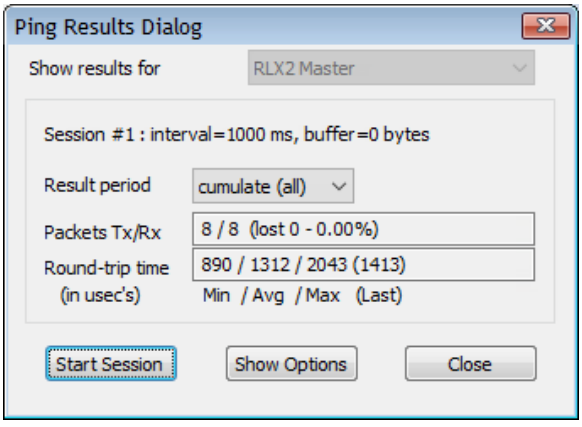
You can use the *Ping* command to test the latency of the network link between the PC running the IH Browser and any other PC that is also running the IH Browser (called *Ping Stations*).

Note: Currently there is no location information when a ping station responds to an IH Browser scan. Therefore, all Ping stations are shown connected to the top main network. It is also possible to select an RLX2/ELXM series radio and start a Ping Session with it.

1. Start the IH Browser on your computer.
2. To start the ping session, do one of the following:
   - From the **VIEW** menu choose **SHOW PING STATIONS**.
   - Click the *Show Browsers* button on the toolbar.



3. Click (highlight) one of the other computers visible in the IH Browser.
4. From the **ACTIONS** menu choose **PING DEVICE** to open the *Ping Results Dialog* box.



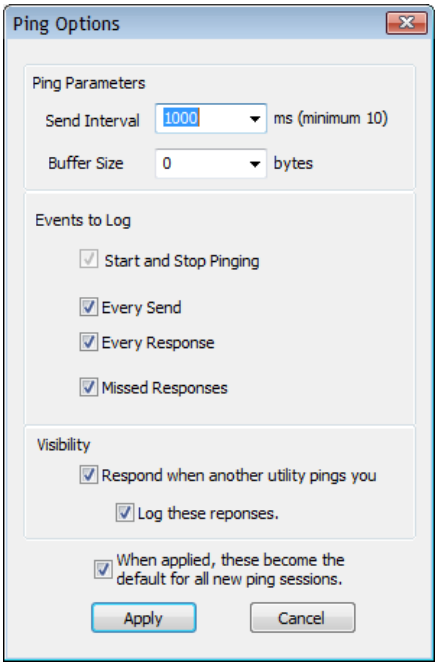
5. This dialog box displays statistics on the minimum, maximum and average latency between two points on the network.

6 Click **SHOW OPTIONS** to change the Ping parameters. For more information, see section *8.1 Setting the Ping Parameters*.

Note: If there is no PC with an IH Browser behind a remote RLX2/ELXM series radio, you can select and ping the radio itself to test its wireless link.

8.1 Setting the Ping Parameters

Use the *Ping Options* dialog box to choose Ping parameters, logging options, and response to other stations.



Parameter	Description
Ping Parameters	
Send Interval	Specifies the time between ping signals in milliseconds. The minimum interval is 10 ms.
Buffer Size	Specifies the buffer size in bytes (the number of bytes sent on the ping).
Events to Log	
Start and Stop Pinging	Logs the beginning and ending of the ping session.
Every Send	Logs every ping signal sent.
Every Receive	Logs every ping response received.
Missed Responses	Logs every missed ping response (when a radio does not respond to a ping signal.
Visibility	
Respond when another utility pings you	Select this check box to reply to a ping request from another radio.
Log these responses	Logs each ping response sent to another radio.
When applied, these become the default for all new ping sessions	Select this check box to use these settings for all future ping sessions with any radio.

9 Viewing Network Data in the IH Browser

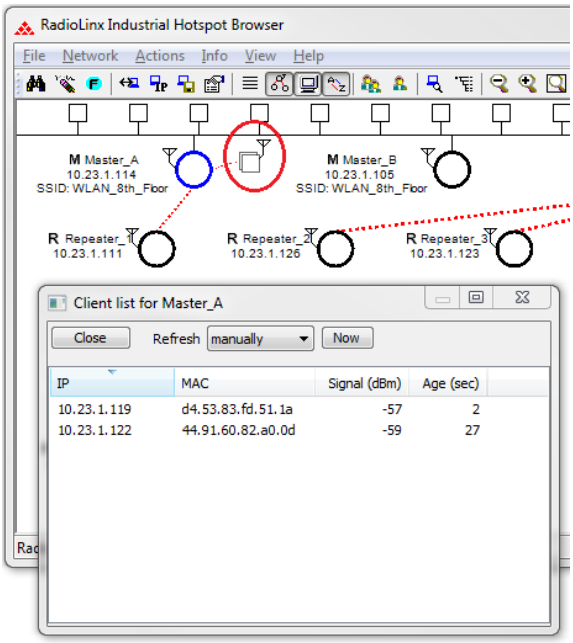
The IH Browser **INFO** feature allows you to monitor the network connections for the selected radio in either the List View or Topology View. The feature shows:

- Wireless clients attached to the radio.
- Information about devices detected via the Ethernet interface of the radio.
- The 802.11 Access Points that are detected by this particular radio.
- The active ports on the radio.

9.1 Viewing Wireless Clients in the IH Browser

The *Client List* dialog box can be opened to show information about wireless clients connected to the currently selected radio. Radios with wireless clients are identifiable as shown by the red outline in the List and Topology Views.

1 In the IH Browser, select a radio in either the *List View* or *Topology View*.
2 From the **INFO** menu choose **WIRELESS CLIENTS**, or right-click the radio and choose **WIRELESS CLIENTS**.

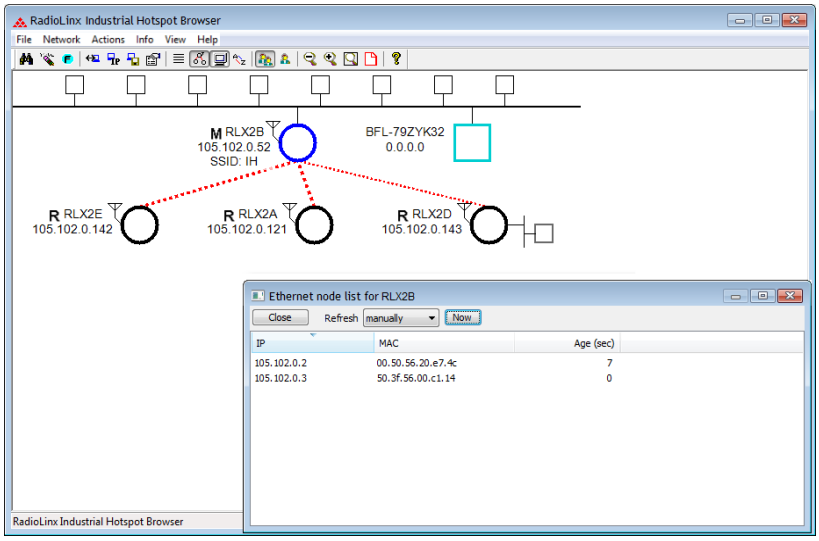


Parameter	Description
Refresh	Data refresh interval in seconds or minutes. Select **MANUALLY** to prevent the IH Browser from automatically updating the data.
Now	Click **Now** to manually update the data.
IP	Displays the IP addresses of the wireless clients connected to the radio.
MAC	Displays the MAC addresses of the wireless clients connected to the radio.
Signal (dBm)	Displays the signal strength from the wireless clients connected to the radio.
Age (sec)	Displays the age of the connection to the wireless clients connected to the radio (the amount of time since a packet has been received from that radio).

9.2 Viewing Ethernet Nodes in the IH Browser

The *Ethernet Node List* dialog box shows information about radios detected by the Ethernet interface to the currently selected radio.

1 In the IH Browser, select a radio in either the *List View* or *Topology View*.
2 From the **INFO** menu choose **ETHERNET NODES**, or right-click the radio and choose **ETHERNET NODES**.



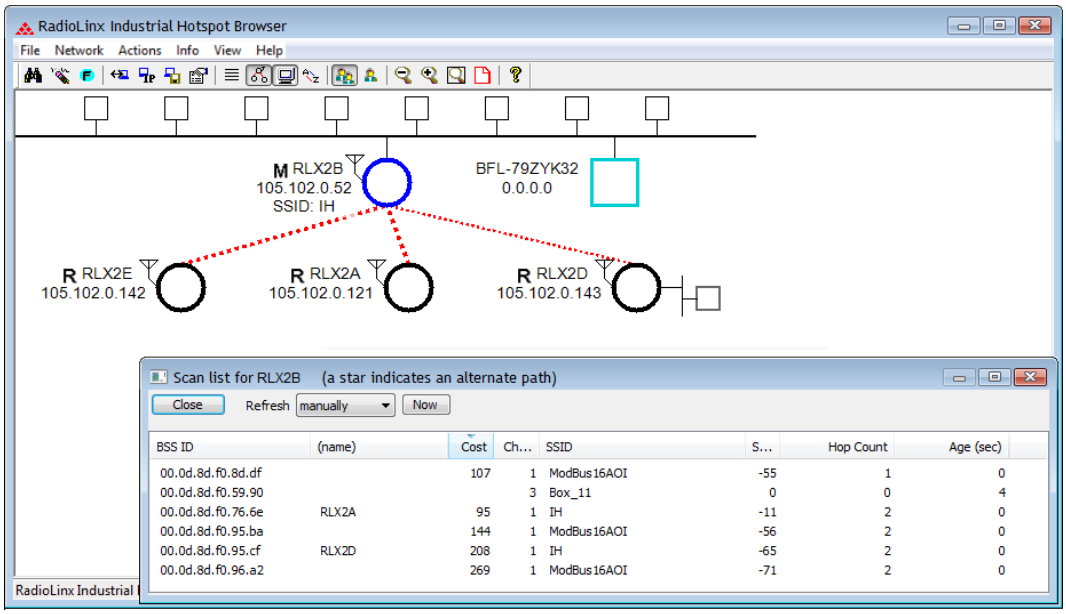
Parameter	Description
Refresh	Specifies the data refresh interval in seconds or minutes. Select **MANUALLY** to prevent the IH Browser from automatically updating the data.
Now	Click **Now** to manually update the data.
IP	Displays the IP addresses of the wireless clients connected to the selected radio.
MAC	Displays the MAC addresses of the wireless clients connected to the selected radio.
Age (sec)	Displays the age of the connection to the wireless clients connected to the selected radio (the amount of time since a packet has been received from that radio).

9.3 Viewing the Scan List in the IH Browser

The *Scan List* dialog box shows all 802.11 Access Points known to the selected radio on this channel (through beacons), even if the Access Point is not linked to the radio (has a different SSID or uses different encryption).

Note: This list shows some of the same information available in the *Available Parents* table in the web interface. For more information, see section *9.6 Viewing Parent Radios in the IH Browser*.

1 In the IH Browser, select a radio in either the *List View* or *Topology View*.
2 From the **INFO** menu choose **SCAN LIST**, or right-click the radio and choose **SCAN LIST**.



List entries marked with an asterisk ***** indicate that the entry is an alternate path, which you can also see if you select the *Parents* button from the toolbar in the *Topology* view (blue lines link the radio to its alternate parents).

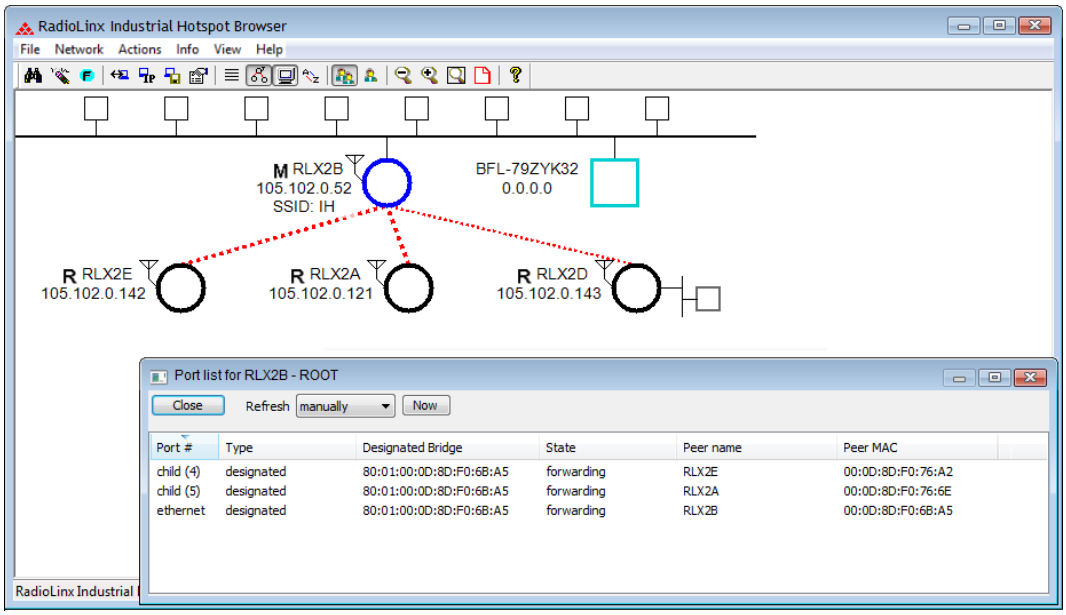
Parameter	Description
Refresh	Specifies the data refresh interval in seconds or minutes. Select **MANUALLY** to prevent the IH Browser from automatically updating the data.
Now	Click **Now** to manually update the data.
BSS ID	Displays the *Basic Service Set Identifier*. This is the MAC addresses of the wireless clients known to the selected radio.
(name)	The name for RLX2/ELXM series radios.
Cost	Displays the calculated parent selection cost. The radio evaluates the link it has to its parent once per second to determine if this link is the best parent to use. The radio calculates the cost for each entry. The cost calculation is based not only on the strongest signal, but on several other factors to provide optimum network communication.
Channel	The radio channel on which the radio is transmitting. The channel list indicates the channel number as well as the frequency (2.4 GHz or 5 GHz bands). **Important:** The RLX2/ELXM series radio is supplied with a dual-band antenna that supports both frequency ranges. If you use a different antenna with the RLX2/ELXM series radio, you must choose a channel and frequency range supported by the antenna.

Parameter	Description
SSID	Displays the network name (Service Set Identifier) of the Ethernet device to which the radio is connected. The radio name appears for RLX2/ELXM series radios.
Signal (dBm)	Displays the strength of the signal from the wireless clients connected to the selected radio.
Hop Count	Displays the number of hops to the Master radio. A value of **0** appears for non-ProSoft Technology devices.
Age (sec)	Displays the age of the connection to the wireless clients connected to the selected radio (the amount of time since a packet has been received from that radio).

9.4 Viewing the Port Table in the IH Browser

The *Port List* dialog box shows all active ports on the selected radio when the Spanning Tree is enabled on the radio.

1 In the IH Browser, select a radio in either the *List View* or *Topology View*.
2 From the **INFO** menu choose **PORT TABLE**, or right-click the radio and choose **PORT TABLE**.



The port table is a list of all the active ports on the radio. Each RLX2/ELXM series radio has up to 252 active ports: one Ethernet wired port, one parent radio frequency link, and up to 250 child radio frequency links.

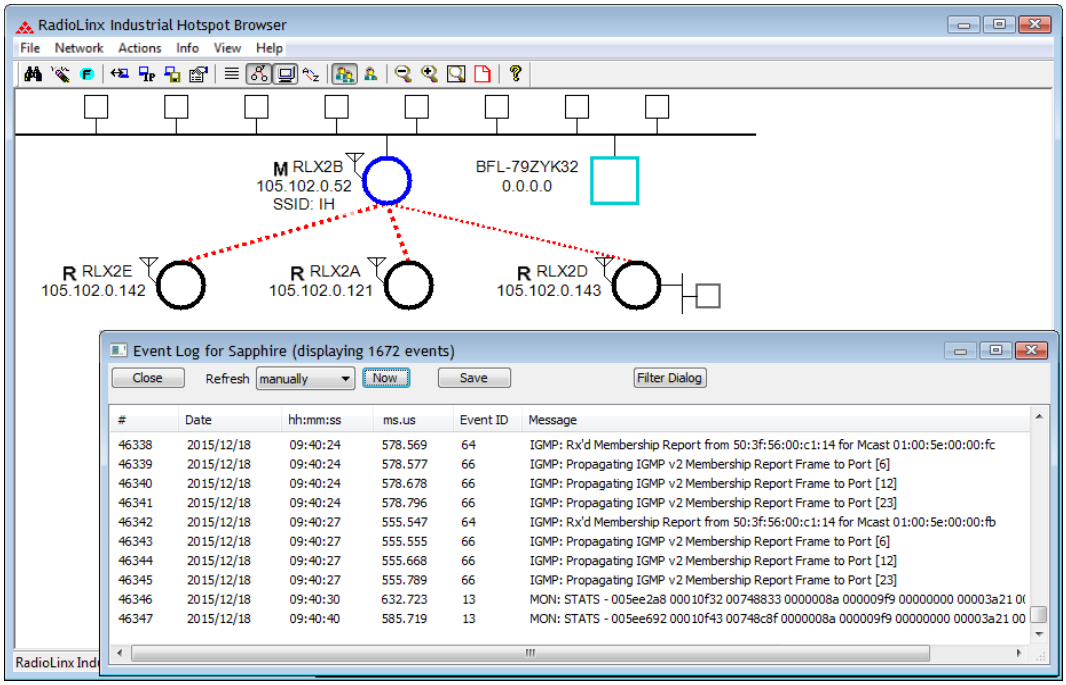
Parameter	Description
Refresh	Specifies the data refresh interval in seconds or minutes. Select **MANUALLY** to prevent the IH Browser from automatically updating the data.
Now	Click **Now** to manually update the data.
Port #	Displays the selected radio's port number.
Type	Displays the type of the port (**ETHERNET PORT**, **PARENT RF LINK**, **CHILD RF LINK**).
Designated Bridge	The next bridge toward the Spanning Tree root for this port.
State	Displays the current Spanning Tree state of the port (**BLOCKING**, **LEARNING**, **LISTENING**, and **FORWARDING**). Forwarding packets can be transferred.
Peer Name	Displays the name of the Master radio if the current radio is a Repeater radio.
Peer MAC	Displays the MAC address of the Master radio if the current radio is a Repeater radio.

9.5 Viewing the Radio Event Log in the IH Browser

The *Event Log* dialog box displays the history of events that have been recorded by the currently selected radio. This can be useful for troubleshooting problems.

1 In the IH Browser, select a radio in either the *List View* or *Topology View*.
2 From the **INFO** menu choose **EVENT LOG**, or right-click the radio and choose **EVENT LOG**.

The Event Log shows the history of a particular radio. You can save the Event Log to a text file for troubleshooting purposes.



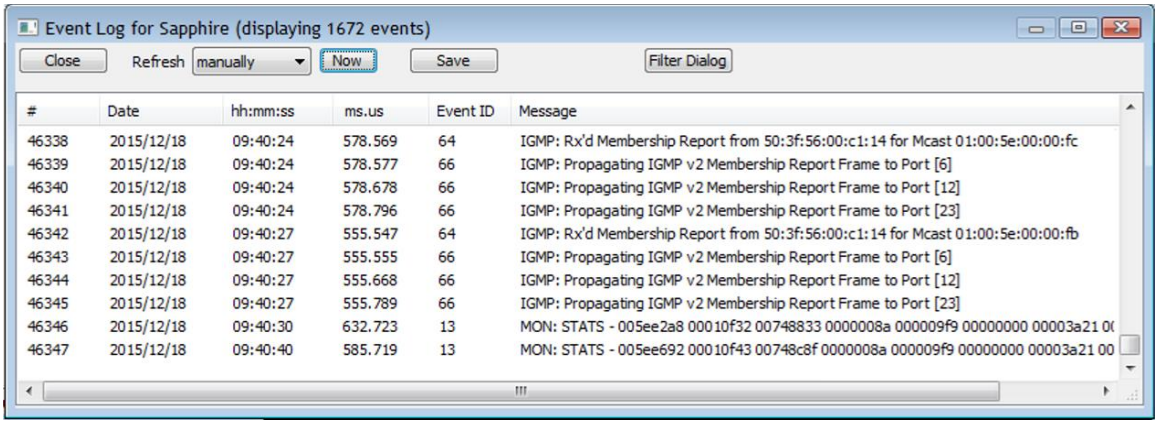
Parameter	Description
Refresh	Specifies the data refresh interval in seconds or minutes. Select **MANUALLY** to prevent the IH Browser from automatically updating the data.
Now	Click **Now** to manually update the data.
Save	Click **SAVE** to save the Event Log to a file for troubleshooting or sending to ProSoft Technology Technical Support.
Filter Dialog	Click **FILTER DIALOG** to change the Event Log filtering to show or hide certain events. For more information, see section *9.5.1 Setting the Event Log Filter*.

9.5.1 Setting the Event Log Filter

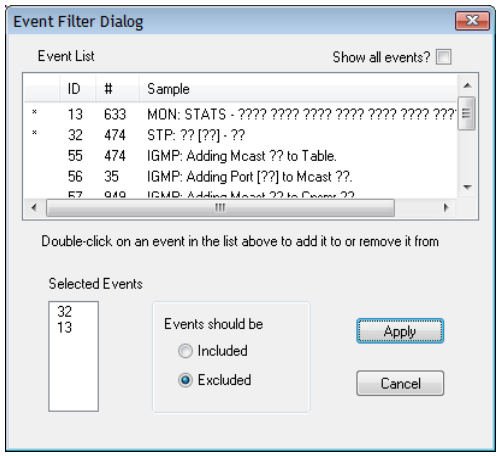
The *Event Filter* dialog box allows you to include or exclude specific event types from the Event Log. The filter conditions that you set in this dialog box affect both the display of events in the *Event Log* dialog box, and the events in the file you create when you click **SAVE** in the *Event Log* dialog box.

Note: The filter conditions are reset to the default state (include all events) when you close the *Event Log* dialog box.

1. In the IH Browser, click on a radio in either the *List View* or *Topology View*.
2. From the **INFO** menu choose **EVENT LOG**, or right-click the radio and choose **EVENT LOG**.
3. In the *Event Log* dialog box, click **FILTER DIALOG**.



4. Double-click on an event in the **EVENT LIST** to add it to the **SELECTED EVENTS** list. An asterisk (*****) appears next to the event types in the *Selected Events* list.



Parameter	Description
Event List	Displays a list of different types of events in the log, sorted by **EVENT ID**. By default, this list only includes event types that are in the radio's Event Log. • Double-click an event type to add it to the *Selected Events* list. • Double-click the event type again to remove it from the *Selected Events* list.

Parameter	Description
Show all events	Select this check box to show all event types, even if the type is not in the radio's Event Log.
Selected Events	Displays the list of selected event types.
Events should be	Specifies whether to include only the selected events, or exclude them. **INCLUDED:** Show only the selected events in the Event Log. **EXCLUDED:** Show all events in the Event Log except the selected events.

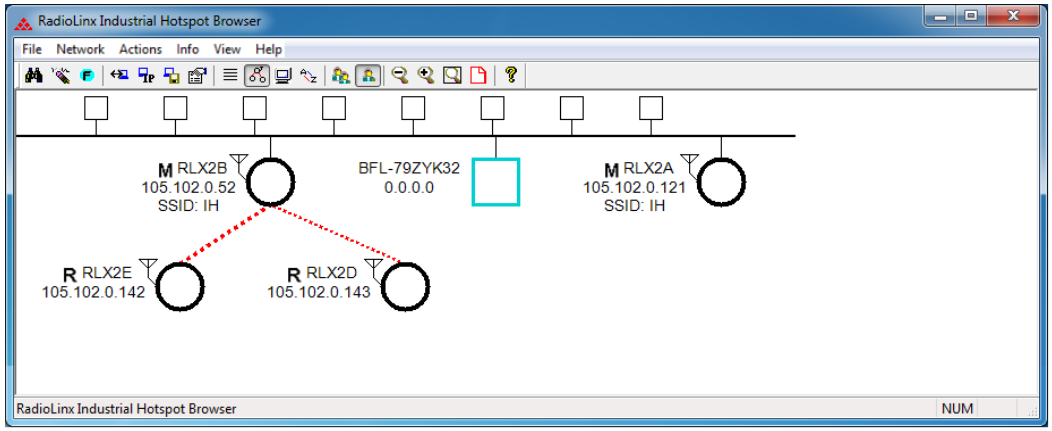
5 You can double-click on the event in the **EVENT LIST** a second time to remove it from the **SELECTED EVENTS** list.

6 Use the **EVENTS SHOULD BE** parameters to include only the selected events, or exclude the selected events.

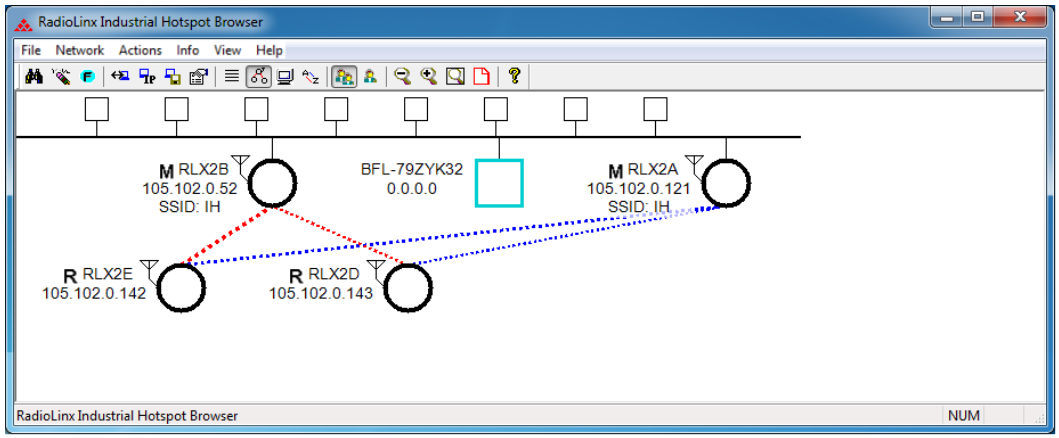
9.6 Viewing Parent Radios in the IH Browser

You can show the current Parent radio or all possible alternate Parent radios for the Repeater radios in the *Topology View*.

- The *Show Selected Parents* button (from the **VIEW** menu choose **SHOW PARENTS - ONE**) shows the link from Repeater radios to their current Parent radio in red.



- The *Show All Parents* button (from the **VIEW** menu choose **SHOW PARENTS - ALL**) shows links to alternate Parent radios in blue (If the Repeater radios can detect other radios in the network). This gives a graphical representation of the number of alternate paths available to a radio should its parent link go down.

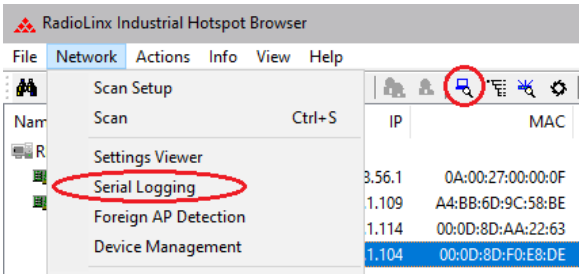


Note: You can also display a detailed list of each of the alternate Parent radios by right-clicking a radio and choosing **SCAN LIST**. This list shows the RLX2/ELXM series radios in the same network and all 802.11 Access Points on other networks. For more information, see section *9.3 Viewing the Scan List in the IH Browser*.

10 Extracting Serial Logs from RLX2/ELXM Radios

This feature allows you to simultaneously retrieve the serial log from multiple RLX2/ELXM series radios, and for an extended period. The serial logs can be used to analyze performance and aid in debugging.

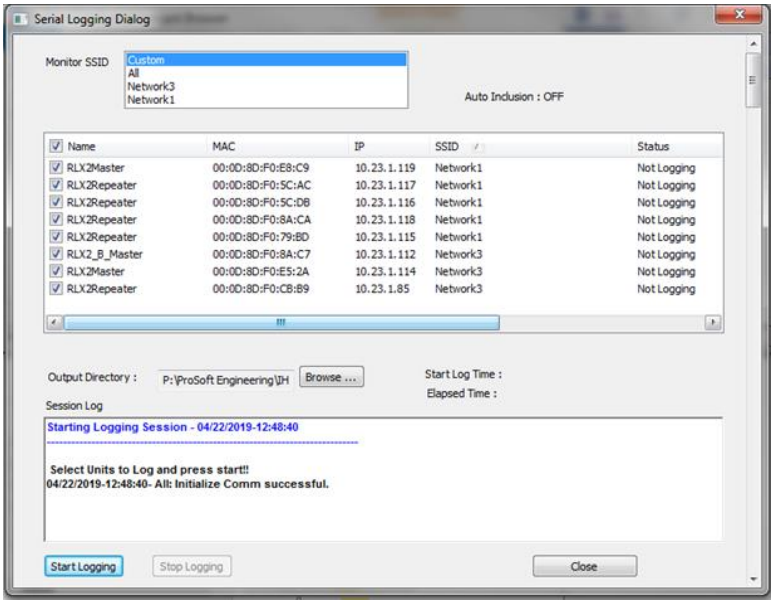
The *Serial Logging Dialog* window can be opened by clicking on **NETWORK** > **SERIAL LOGGING**, or by clicking the **LOGGING** icon in the shortcuts bar.



10.1 Serial Logging Dialog

When the *Serial Logging Dialog* window is opened, all detected RLX2/ELXM series radios in the network are listed. By default, all of the radios are selected to be part of the logging session. The *Monitor SSID* parameter is set to **Custom** as shown in the figure below.

Note: Only radios that are on the same subnet as the IH Browser PC will be able to participate in the logging session.



10.1.1 Monitor SSID

The *Monitor SSID* parameter has three options to select which RLX2/ELXM series radios to be included in the logging session.

Monitor SSID option	Description
Custom	Manually selects each RLX2/ELXM series radio from the list to be included in the logging session
All	Selects all RLX2/ELXM series radios in the list
Specific SSID	Selects the RLX2/ELXM series radios by SSID

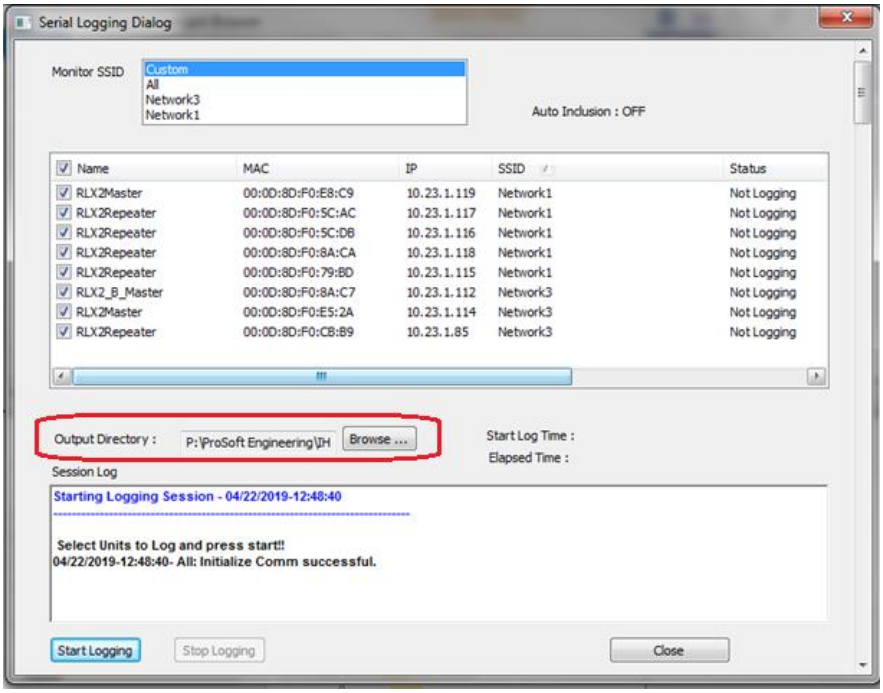
The columns are sortable by clicking on the column header. You can also utilize a group selection by using the standard 'Shift' key method.

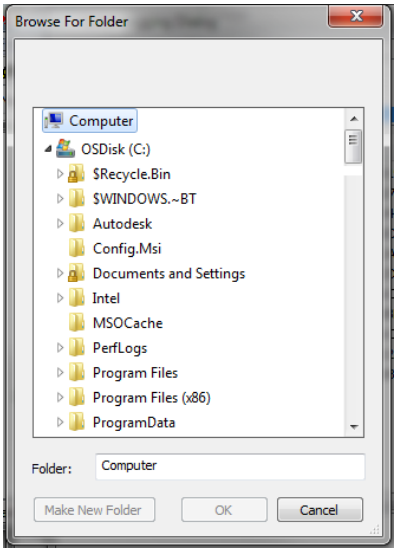
The *All* and *Specific SSID* options automatically enable the *Auto Inclusion* feature. This adds an RLX2/ELXM series radio that is discovered by the IH Browser after a logging session has started. For the *Specific SSID* option, it must also have the same SSID that was selected.

The *Custom* option disables the *Auto Inclusion* feature and only the selected RLX2/ELXM series radios will be included.

10.1.2 Output Directory

Select the file location to store the *Serial Logging Dialog* files by clicking on the **BROWSE** button in the *Output Directory* parameter.

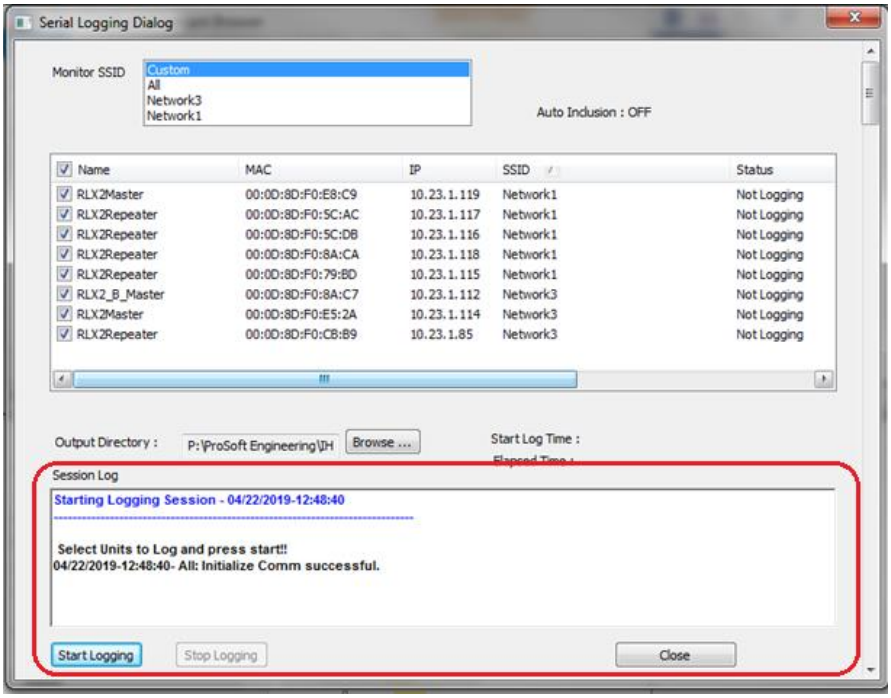




Within the base output directory, a separate subdirectory of active logs for each 24 hour day is created (**mm.dd.yyyy**).

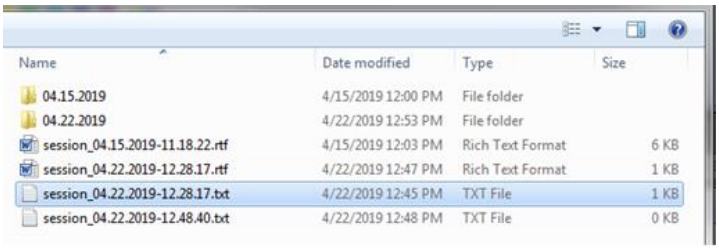
10.1.3 Session Log

The *Session Log* is located at the bottom of the *Serial Logging Dialog*. It contains a session log of all the events and state changes that took place during logging.



The *Session Log* is saved to the base *Output Directory* with the following format:
session_mm.dd.yyyy-hh.mm.ss.txt

Example: session_03.06.2019-13.56.39.txt
The date and time in the session log name is the time that the Session was started (i.e. the Dialog was opened).

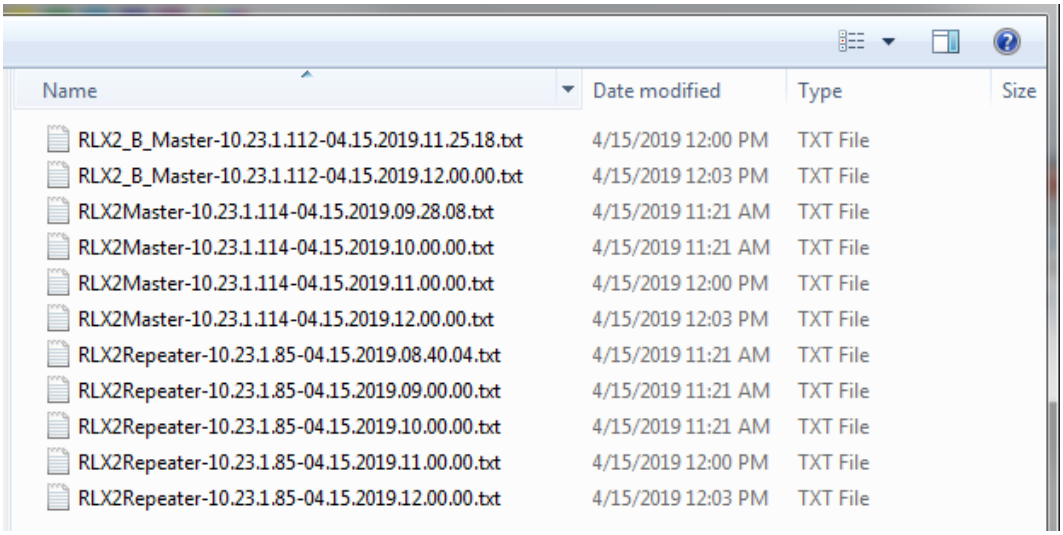


Within the daily directories the individual hourly logging file will be created with the following format:

APname-IPaddr-mm.dd.yyyy.hh.mm.ss.txt

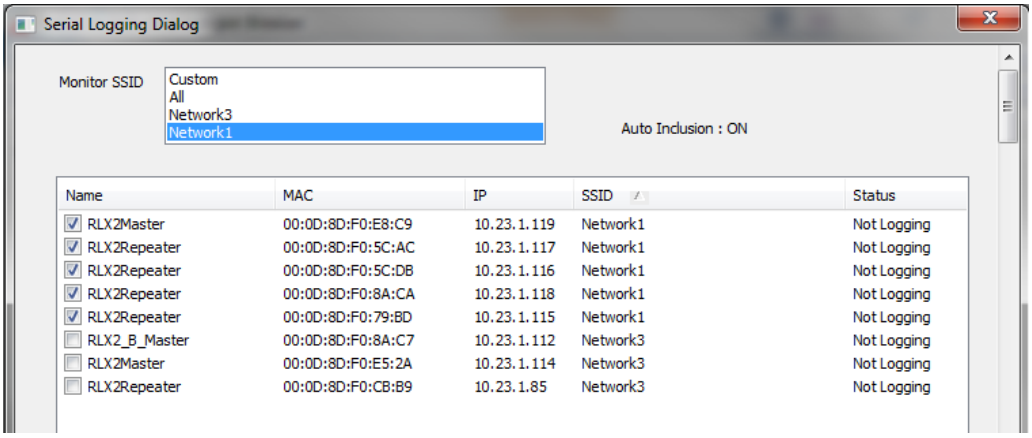
Example: RLX2Master-10.23.1.111-03.01.2019.03.00.00.txt

The time in the first file's name will be the time of the oldest print in the backlog, downloaded after a telnet session is started. New files are created on the hour.

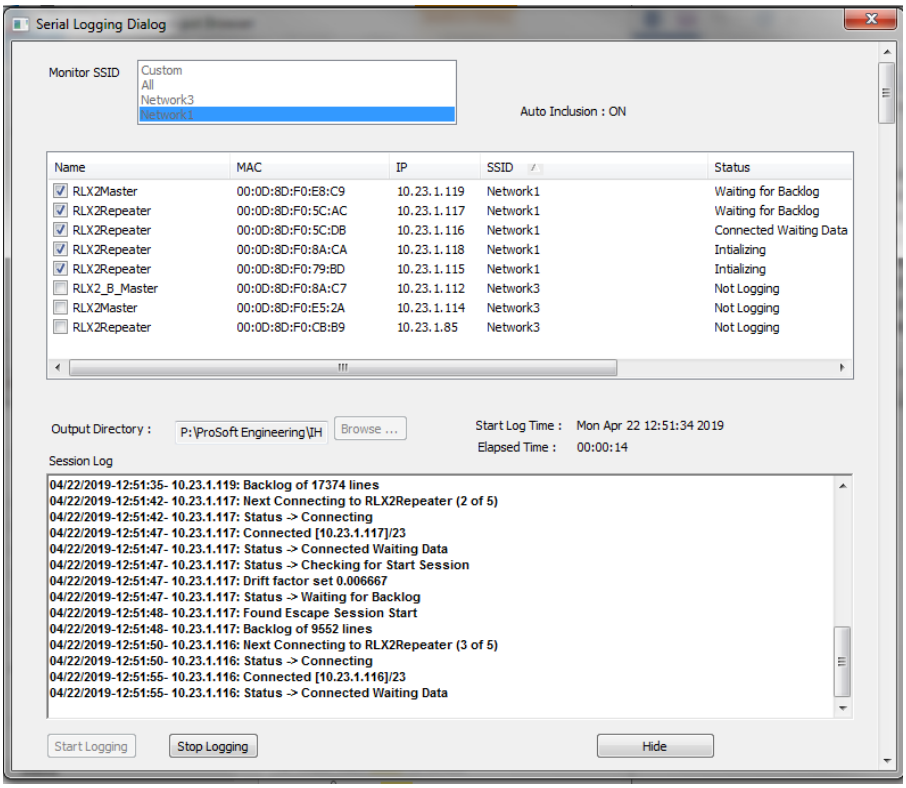


10.2 Starting the Logging Session

In the example below, all RLX2/ELXM series radios that use the **Network1** SSID will be logged.



1. Click the **START LOGGING** button at the bottom of the dialog. The **STOP LOGGING** button activates once logging is started.
2. While logging, you can hide the *Serial Logging Dialog*. It can be brought forward by clicking on **NETWORK** > **SERIAL LOGGING**, or by clicking the **LOGGING** icon in the shortcuts bar.
3. When logging starts, the *Session Log* window lists all events and actions taken by the Logging Session.

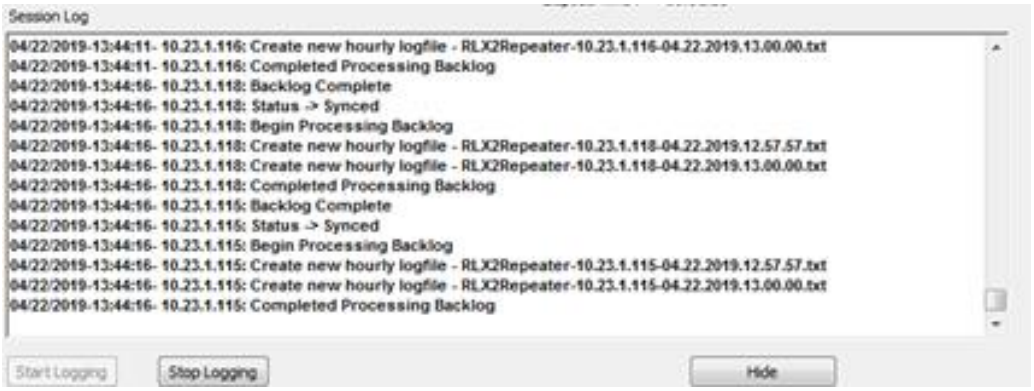


Each of the radios in the session indicates one of the following states in the *Status* column:

State	Description
"Not Logging"	The radio is not selected for logging.
"Initializing"	The radio is selected for logging.
"Connecting"	Attempting to connect to the radio.
"Connected Waiting Data"	Connected to the radio and waiting to receive first data.
"Waiting for Backlog"	Has received data from the radio and now waiting to receive the acculmulated backlog.
"Synced"	The backlog has been received and is fully time synced.
"Stopping"	The utility is stopping its logging session to the radio.
"Resyncing"	The time sync is being reestablished (occurs every hour).
"Reconnecting"	Attempting to reconnect to the radio.
“Failed”	The radio experienced some failure, should attempt to reconnect.
"NoRx"	No Data received in the previous 5 sec period (not an error).
"Failed - Stopped"	The logging session to that unit has failed.

By design, the logging of each RLX2/ELXM series radio is staggered. Approximately one radio connects every 10 seconds. When a radio is first connected, there are up to 20,000 lines of historical backlog in the radio that will all be retrieved by the IH Browser.

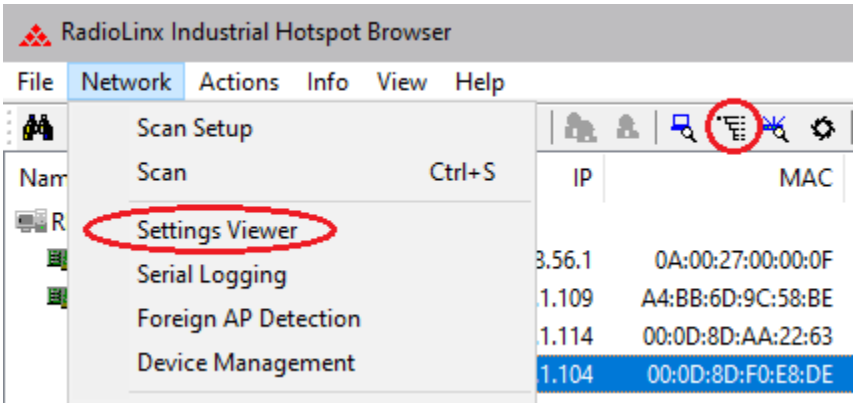
Once this backlog is fully downloaded, the utility will calculate a time sync so that the log entries can be timestamped accurately:



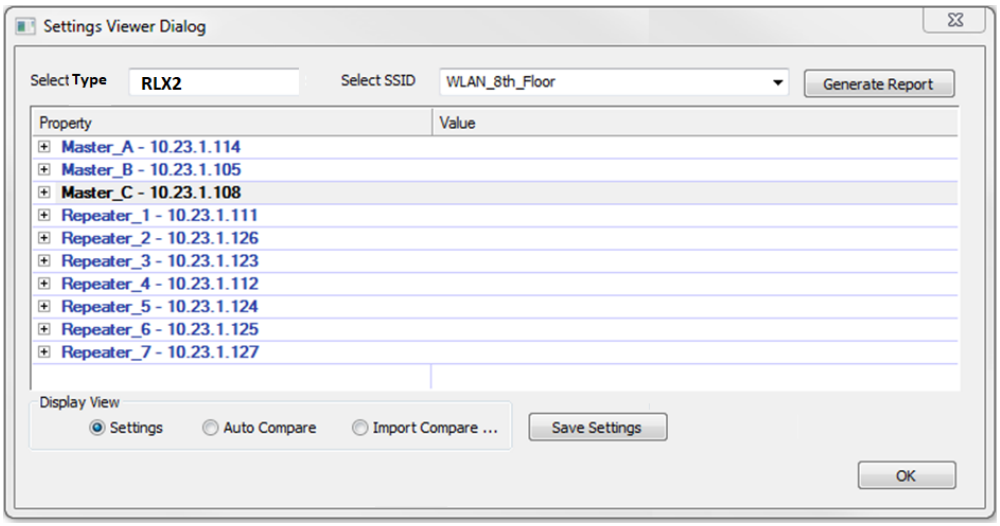
11 Settings Viewer

This feature allows you to view the current settings of RLX2/ELXM series radios on the network. The RLX2 must be running firmware *RLX2_v0037F_R* or later to use this feature and is supported in all ELXM firmware versions.

The *Settings Viewer Dialog* window can be opened by clicking on **NETWORK** > **SETTINGS VIEWER**, or by clicking the **SETTTINGS VIEWER** icon in the shortcuts bar.



All detected radios on the network are listed in the *Settings Viewer Dialog* window. The view is updated automatically each time the IH Browser detects a new radio on the network.

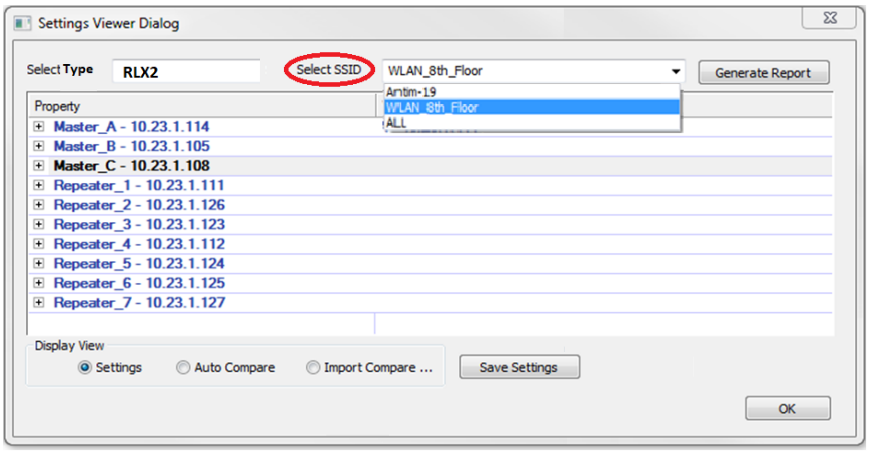


11.1 Select Type

The *Select Type* option filters the available radios of a common network, as identified by their Product Type, **RLX2** or **ELXM**.

11.2 Select SSID

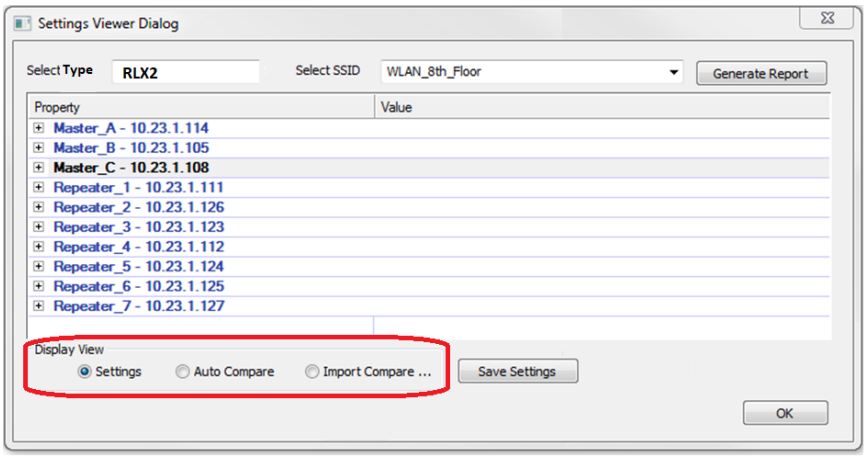
The *Select SSID* option filters the available radios of a common network, as identified by their SSID. The **ALL** option displays all radios detected, regardless of their SSID. The list will be empty for an SSID that does not have any radios of the **Type** selected.



11.3 Display View

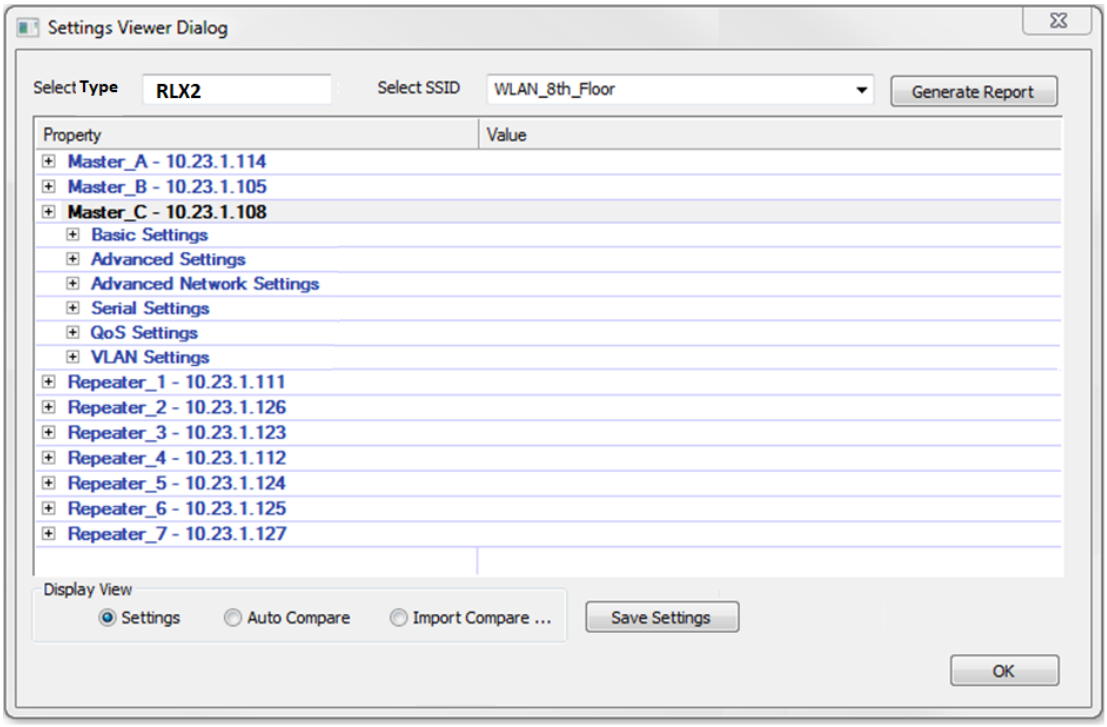
The *Settings Viewer Dialog* window has three different views:

- The **Settings** view displays the current setting values of any radio.
- The **Auto Compare** view compares the settings of the displayed units by grouping them and highlighting the differences.
- The **Import Compare** view compares the settings of the displayed units against settings that were previously saved using the **SAVE SETTINGS** button. This mode is useful in quickly determining if any unit has been inadvertently changed.



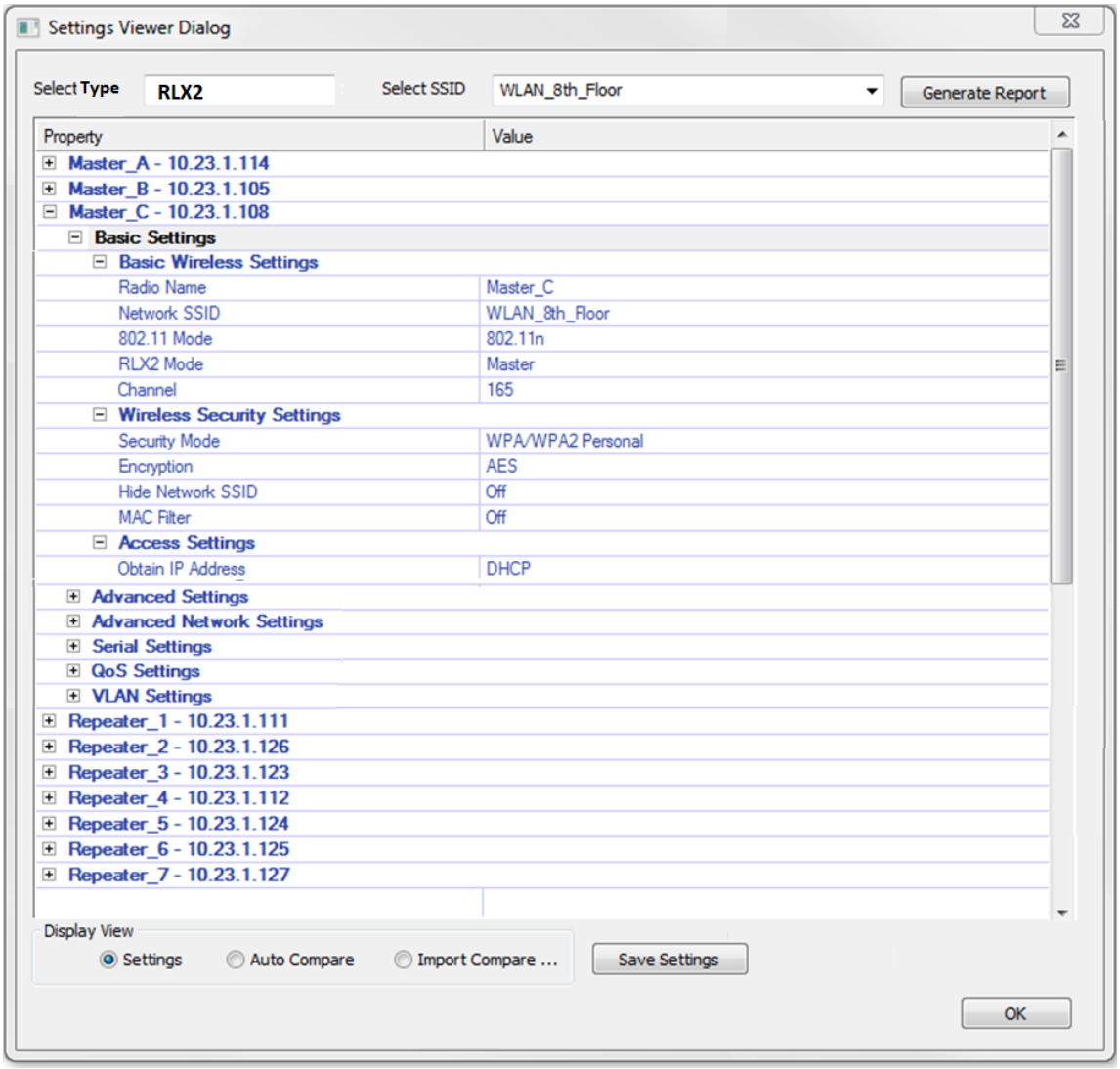
11.4 Settings Viewer

The *Settings Viewer* allows you to browse the current settings of a radio. Clicking on the "**+**" symbol expands the parameter list. The same can be achieved by double-clicking anywhere in a row that has a "**+**" symbol.

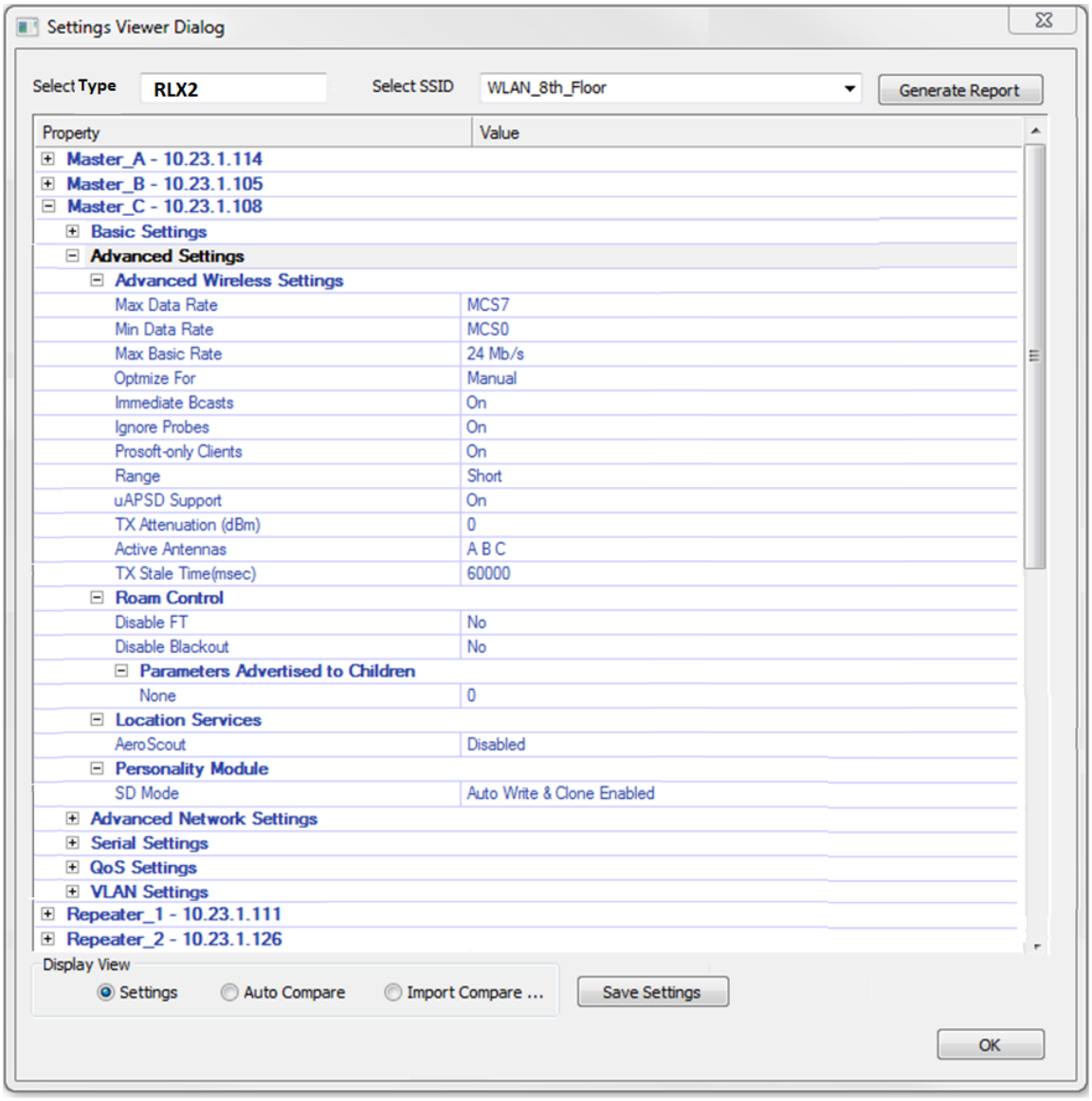


The revealed sub-groups match the tabs of the radio's web interface.

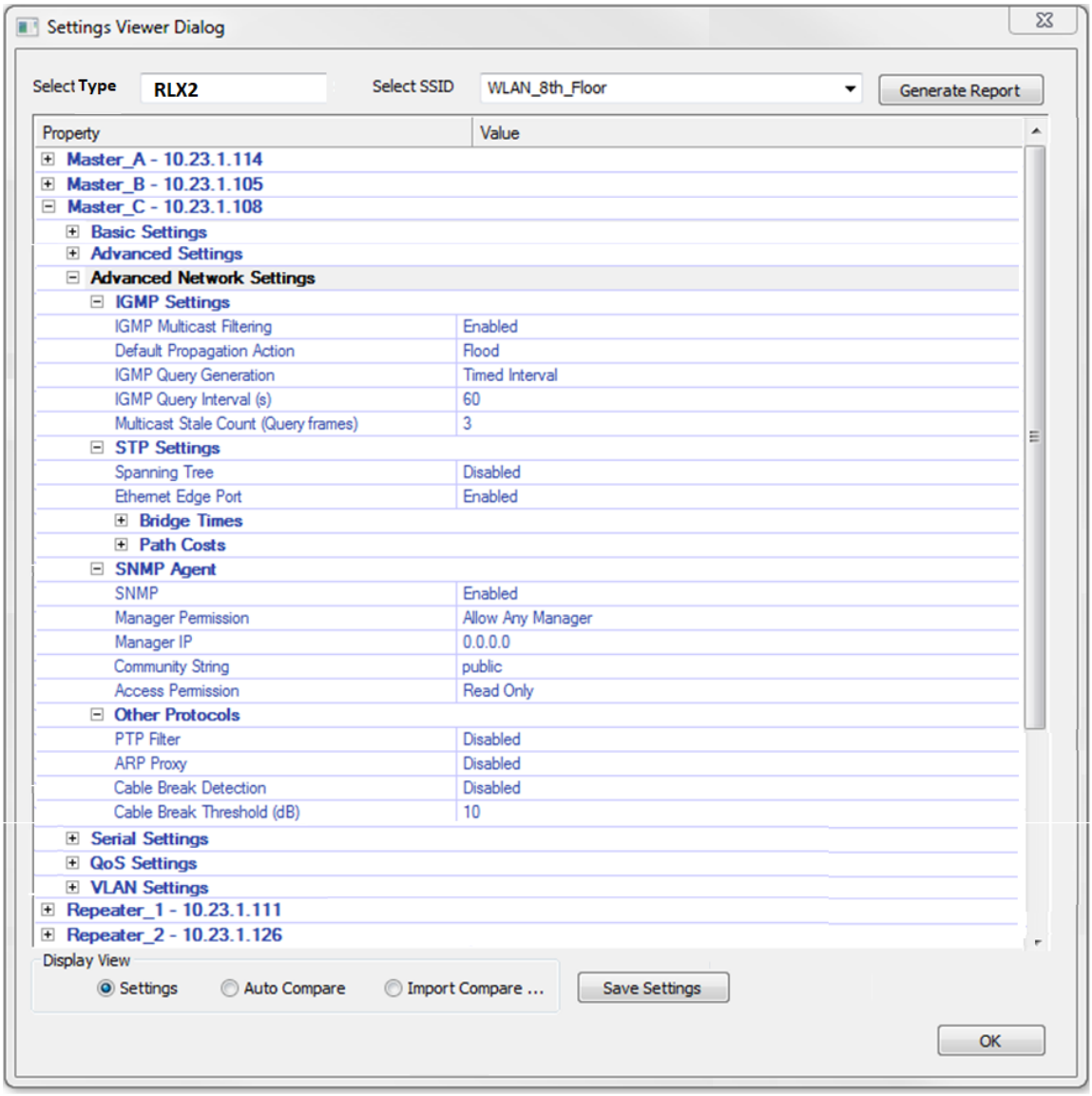
11.4.1 Basic Settings



11.4.2 Advanced Settings



11.4.3 Advanced Network Settings



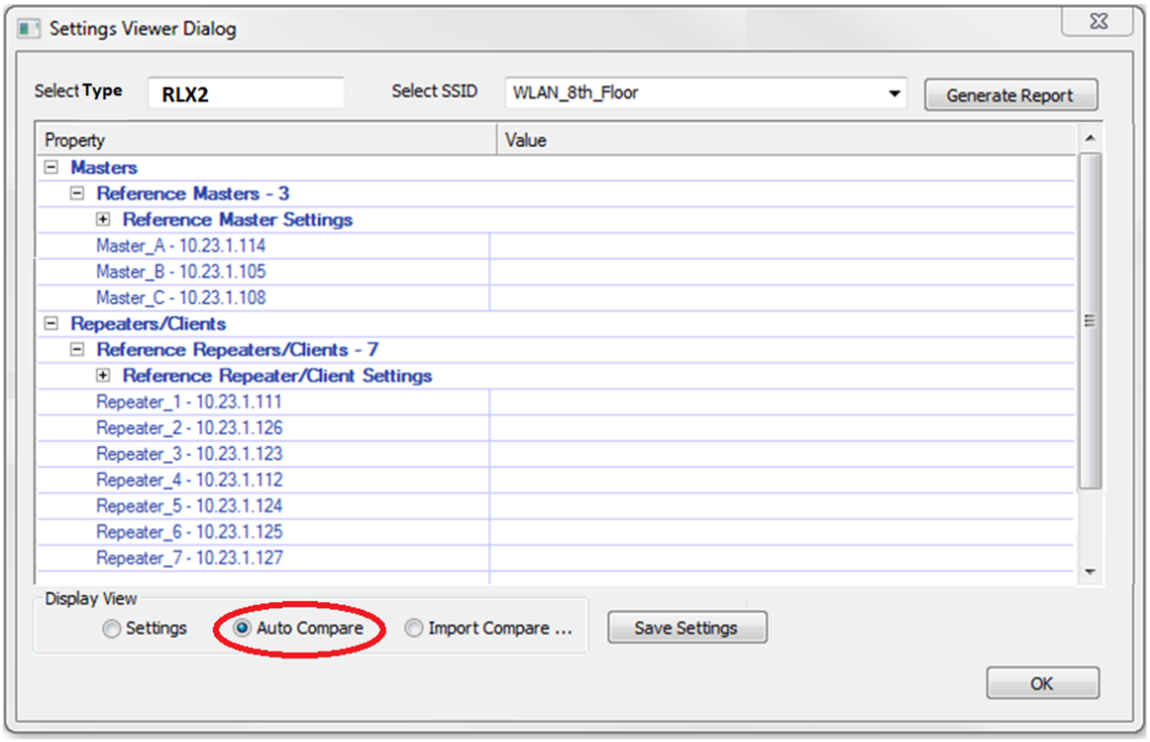
11.5 Auto Compare View

The *Auto Compare* view compares the settings of the displayed units by grouping them and highlighting the differences. Repeaters are only compared against other Repeaters, and Masters against other Masters.

The largest group of Repeaters and the largest group of Masters with common settings becomes the **Reference.** The differences between the Repeaters/Masters and their respective References are displayed.

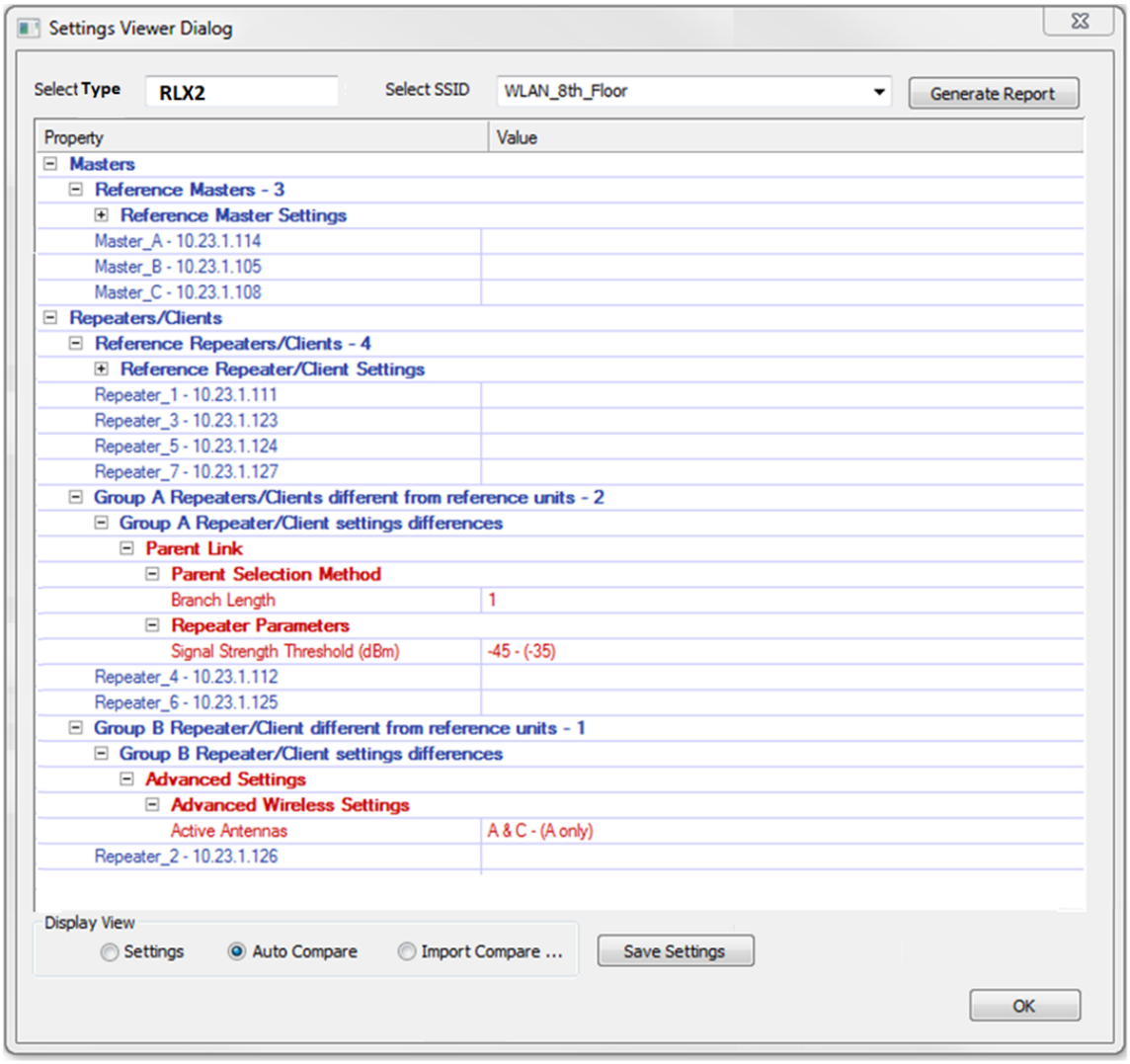
The example below shows that all units have the same settings. All Repeaters are a part of the Reference Repeater group and all Masters are a part of the Master Reference group.

You can browse the settings by expanding (**+**) the *Reference xxx Settings* groups.



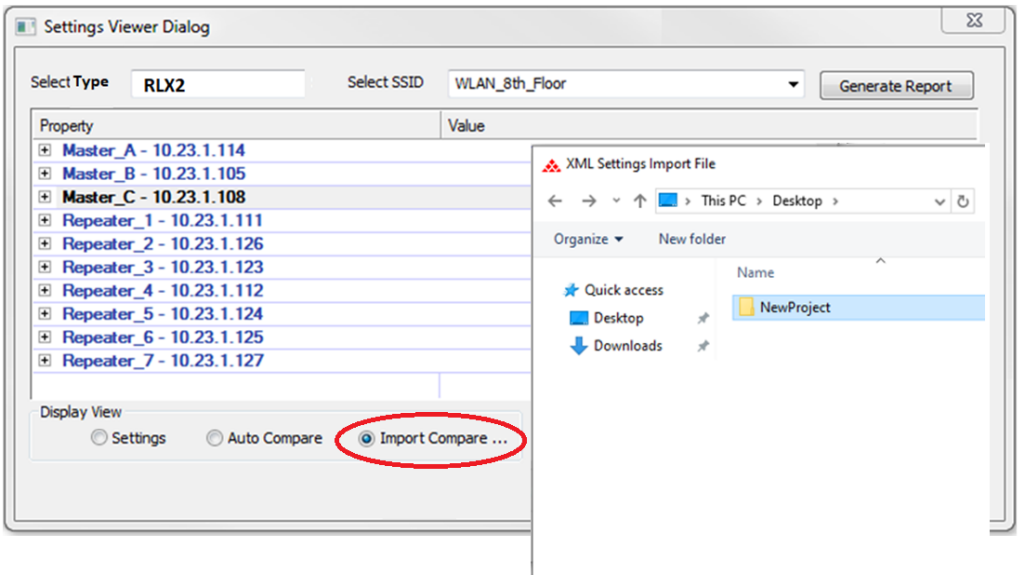
The example below shows three Repeaters that have setting differences from the **Reference Repeaters**. Two of the Repeaters have the same differences and are displayed in their own group labeled **Group A**. Another Repeater has an additional difference from the **Reference Repeaters** and is labeled **Group B**.

In these difference groups, only the settings that are different are shown and highlighted in red. Where possible, the Reference value for the setting is shown in brackets.



11.6 Import Compare

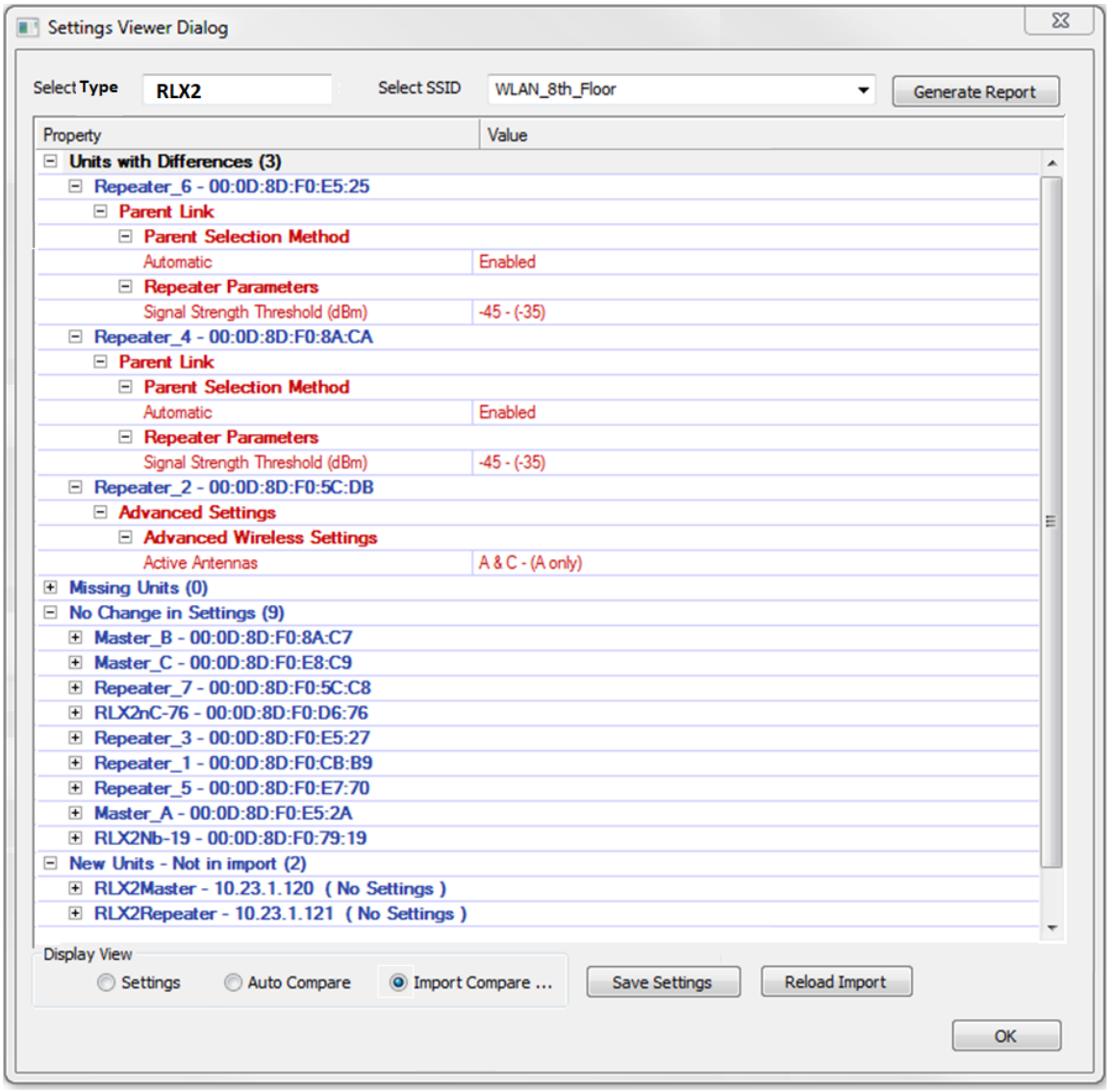
The *Import Compare* button allows you to select a previously saved *.settings* file.



Once the file is selected, the settings of the radio that have been discovered by the IH Browser are compared against the settings of the radio in the imported settings file.

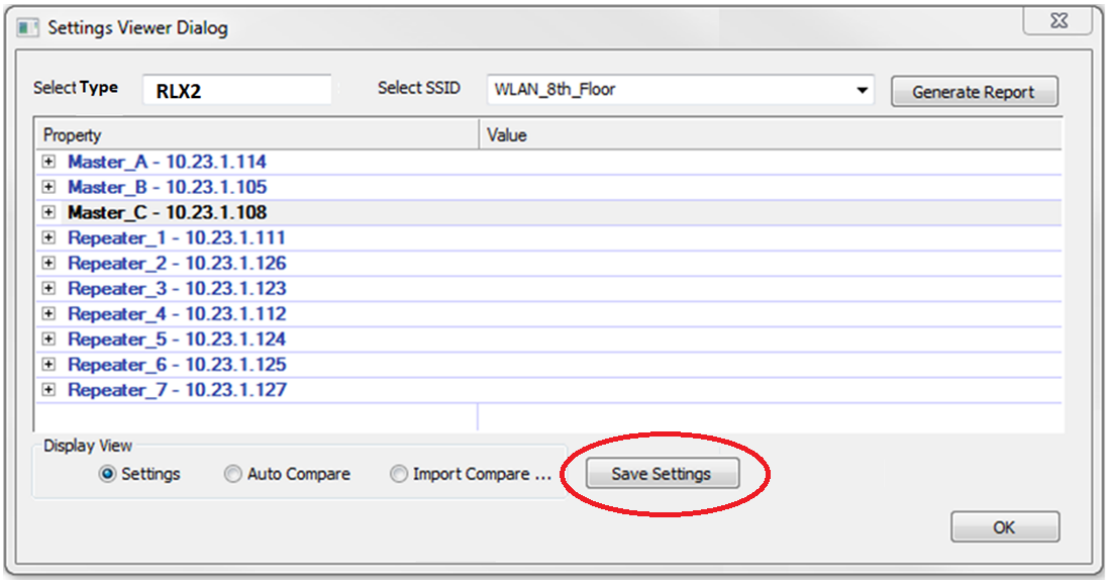
The comparison results are separated into 4 groups:

- **Units with Differences**
  - Units that have one or more different settings than the settings previously saved.
  - The setting differences are highlighted in red.
- **Missing units**
  - Units that were in the import file but not currently discovered by IH Browser.
- **No Change in Settings**
  - Units whose settings are exactly the same as in the imported settings file.
- **New Units**
  - Units that are currently present but are not in the imported settings file.

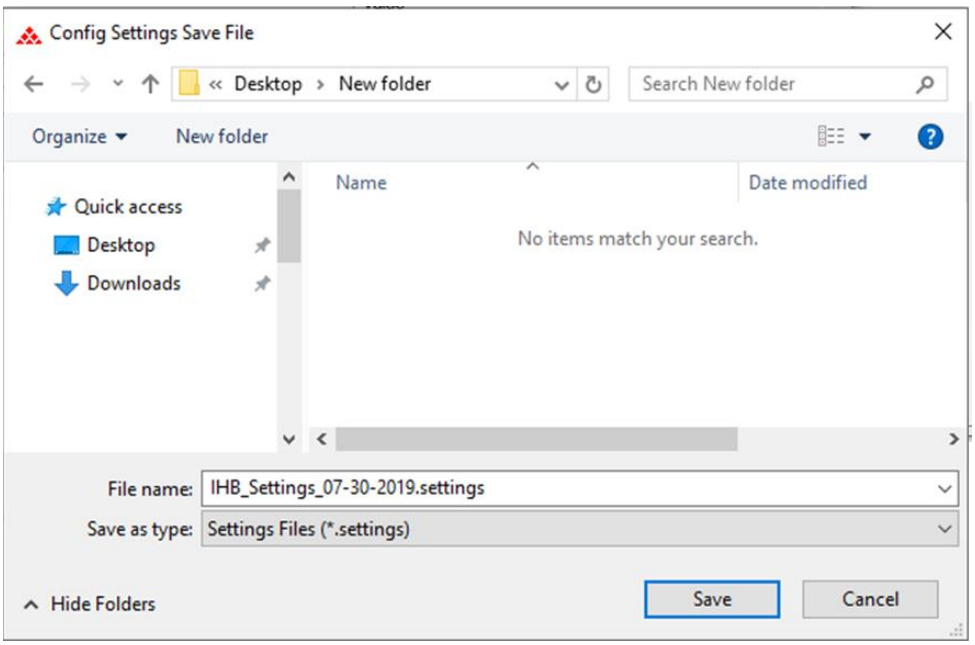

Settings Viewer Dialog
Select Type
RLX2
Select SSID
WLAN_8th_Floor
Generate Report
Property
Value
Units with Differences (3)
Repeater_6 - 00:0D:8D:F0:E5:25
Parent Link
Parent Selection Method
Automatic
Enabled
Repeater Parameters
Signal Strength Threshold (dBm)
-45 - (-35)
Repeater_4 - 00:0D:8D:F0:8A:CA
Parent Link
Parent Selection Method
Automatic
Enabled
Repeater Parameters
Signal Strength Threshold (dBm)
-45 - (-35)
Repeater_2 - 00:0D:8D:F0:5C:DB
Advanced Settings
Advanced Wireless Settings
Active Antennas
A & C - (A only)
Missing Units (0)
No Change in Settings (9)
Master_B - 00:0D:8D:F0:8A:C7
Master_C - 00:0D:8D:F0:E8:C9
Repeater_7 - 00:0D:8D:F0:5C:C8
RLX2nC-76 - 00:0D:8D:F0:D6:76
Repeater_3 - 00:0D:8D:F0:E5:27
Repeater_1 - 00:0D:8D:F0:CB:B9
Repeater_5 - 00:0D:8D:F0:E7:70
Master_A - 00:0D:8D:F0:E5:2A
RLX2Nb-19 - 00:0D:8D:F0:79:19
New Units - Not in import (2)
RLX2Master - 10.23.1.120 (No Settings)
RLX2Repeater - 10.23.1.121 (No Settings)
Display View
Settings
Auto Compare
Import Compare ...
Save Settings
Reload Import
OK

11.7 Save Settings Button

You can save the settings of all units that are known by the IH Browser so that they can be used as a reference when doing an “Import Compare”.

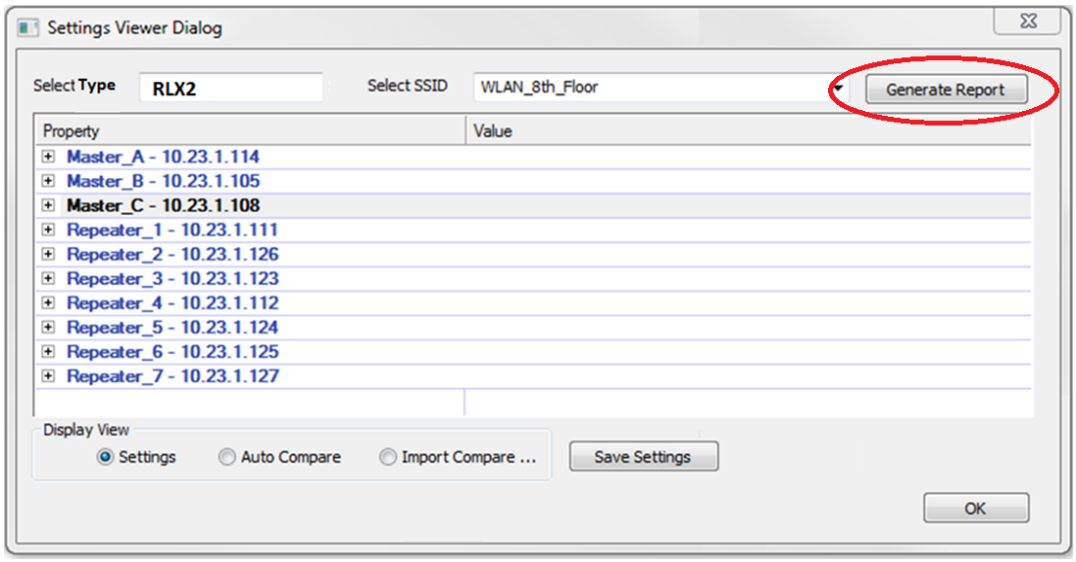


The **SAVE SETTINGS** button allows you to select the folder to save the *.settings* file. The default file name is: “IHB_Settings_*dd_mm_year*.settings”.

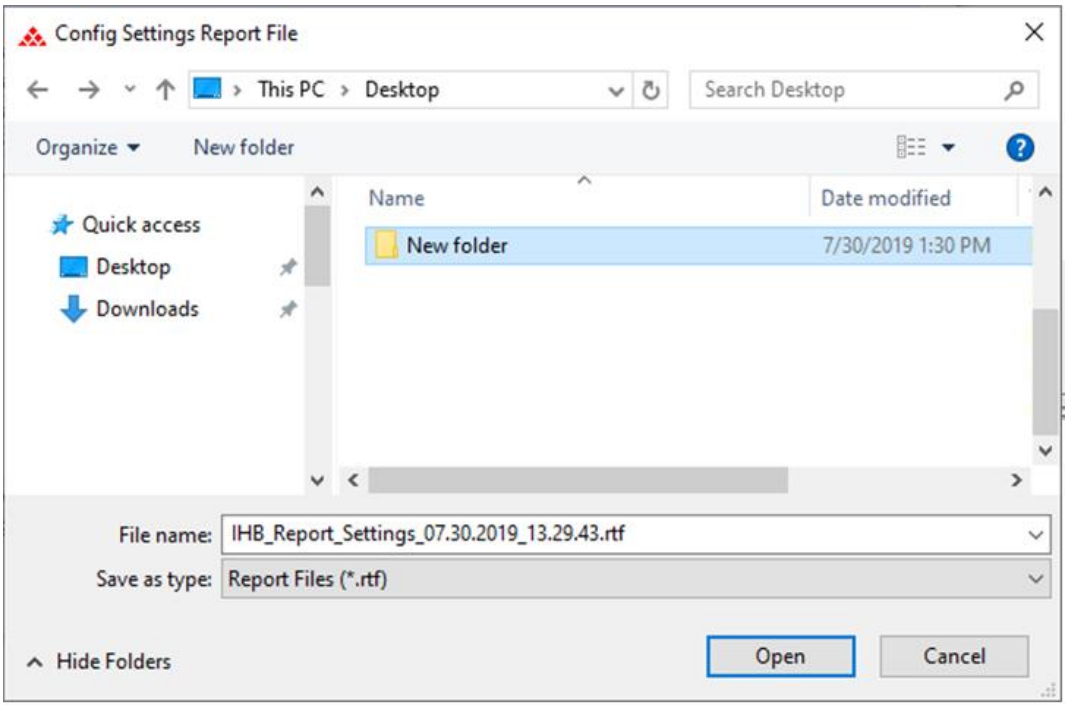


11.8 Generate Report Button

You can create a Word document that contains an expanded view of all the unit settings by clicking on the **GENERATE REPORT** button.



The **GENERATE REPORT** button allows you to select the folder to save the *.rtf* file. The default file name is: "IHB_Report_Settings_*mm.dd.year_hh.mm.ss*.rtf".



11.8.1 Example Report

Display Settings Report

RLX2 - 192.168.2.201

Basic Settings

Basic Wireless Settings

Radio Name	: RLX2
Network SSID	: Network1
802.11 Mode	: 802.11n
RLX2 Mode	: Master
Channel	: 48

Wireless Security Settings

Security Mode	: WPA/WPA2 Personal
Encryption	: AES
Hide Network SSID	: Off
MAC Filter	: Off

Access Settings

Obtain IP Address	: DHCP

Advanced Settings

Advanced Wireless Settings

Max Data Rate	: 54 Mb/s
Min Data Rate	: MCS0
Max Basic Rate	: 24 Mb/s
Optmize For	: RLX2 Bridging
Immediate Bcasts	: On
Ignore Probes	: On
Prosoft-only Clients	: Off
Range	: Long
Range (km)	: 25
uAPSD Support	: On

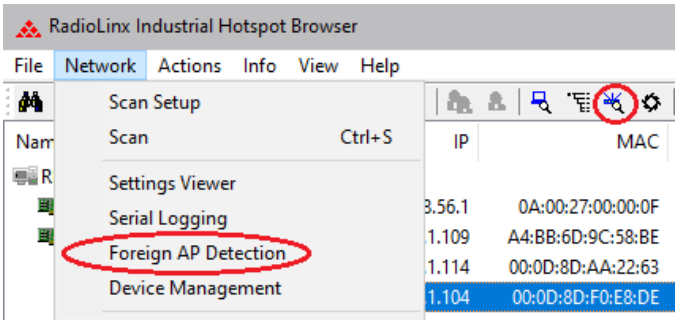
12 Foreign AP Detection

This feature retrieves scan information from radios that have responded to the IH Browser and appear in the main list view. This scan data can be used to detect the presence of rogue foreign Access Points that are operating on the same channel as the radios and can become a source of serious interference.

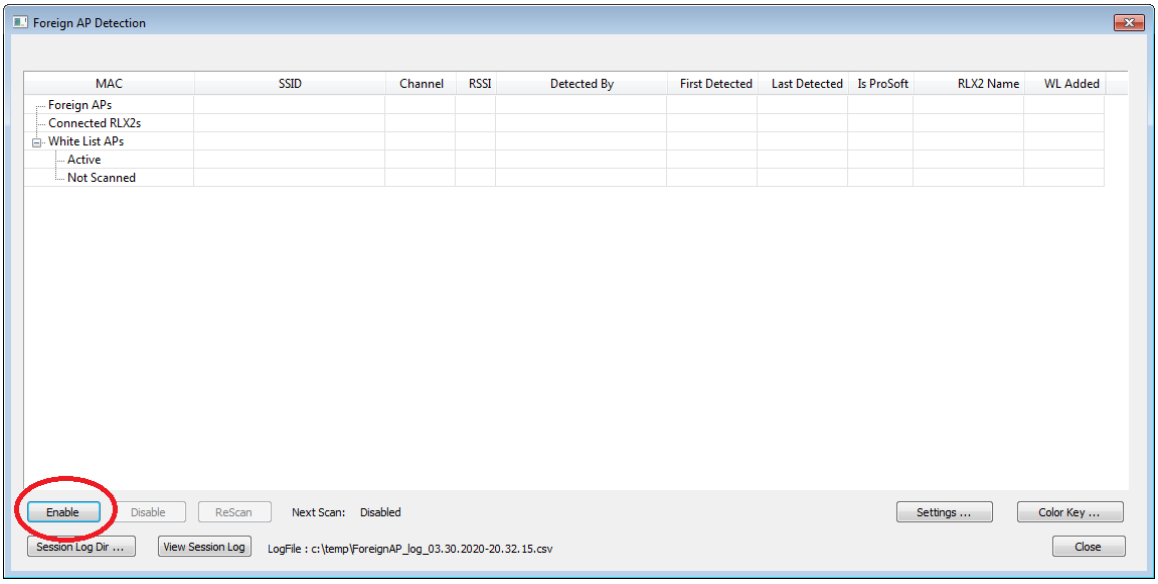
The IH Browser maintains a whitelist which allows the IH Browser to differentiate between detected APs that are meant to be present on that channel and APs that have come online in the facility either by error, or with malicious intent. A **foreign AP** is therefore defined as any AP that is not in the whitelist.

12.1 Navigation

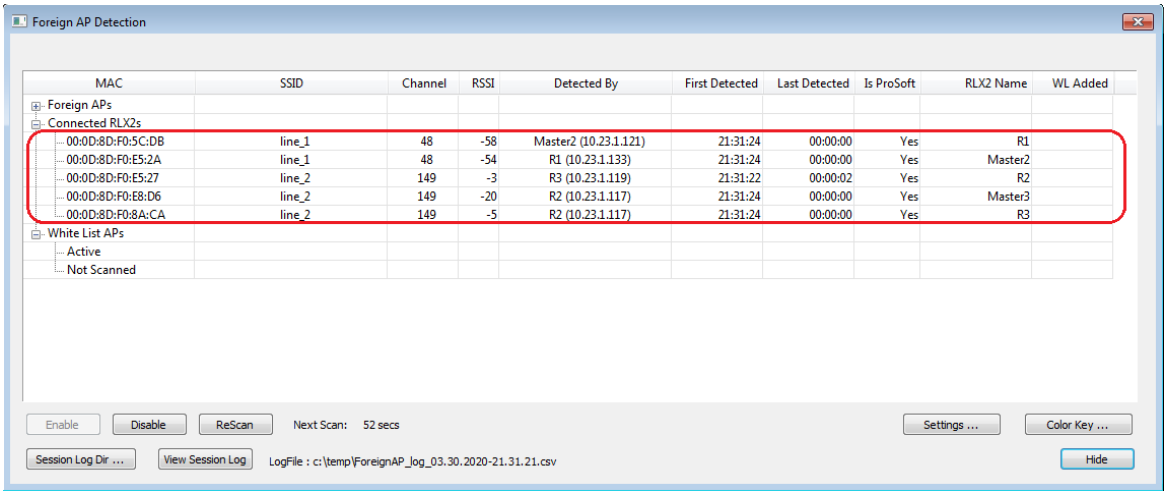
The *Foreign AP Detection* dialog window can be opened by clicking on **NETWORK** > **FOREIGN AP DETECTION**, or by clicking the **FOREIGN AP DETECTION** icon in the shortcuts bar.



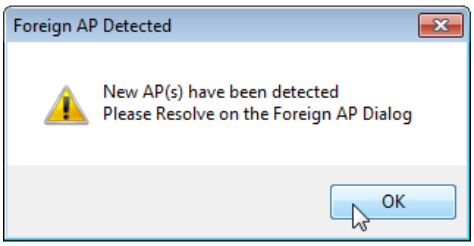
The dialog window initially opens in the disabled state as shown below. Clicking on the **ENABLE** button will enable the feature and the IH Browser will commence pulling scan information from the radios.

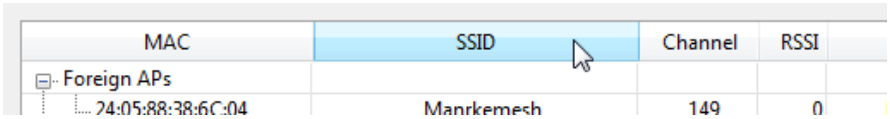


When first enabled the dialog populates the **Connected RLX2s** section of the display with all radios (including ELXM radios) that are present in the main view of the IH Browser. These are the radios that will be used as a source of Scan information to populate the other sections of the display.

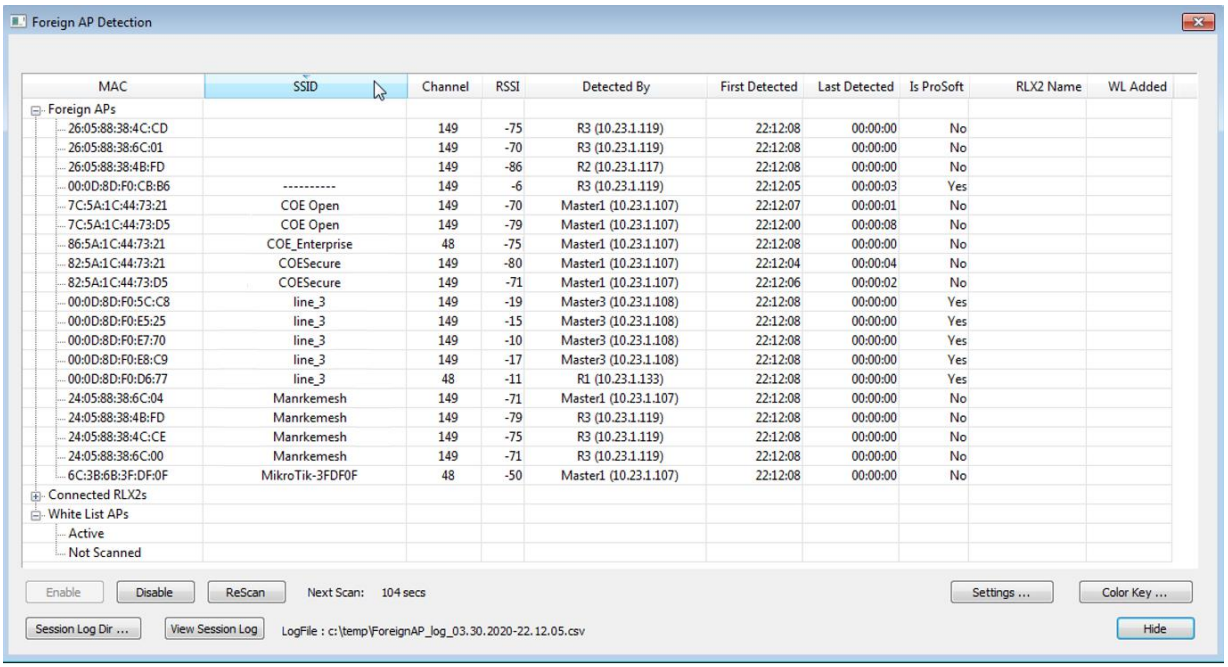


When any Foreign APs are detected the following pop up appears. Clicking the **OK** button will expand the **Foreign APs** section and display all APs that have currently been detected.



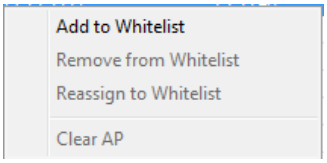


In the *Foreign AP Detection* dialog shown in the example below, the whitelist is currently empty as we have not yet assigned the known good APs to the whitelist. Therefore all detected APs are initially displayed in the Foreign APs section.



Column	Description
MAC	MAC address of the AP.
SSID	The SSID that the AP is advertising in its Beacon.
Channel	The channel number on which the AP was detected.
RSSI	The signal strength of the AP as measured by the detecting unit. **Note:** If more than one radio has detected the device the table will display the information from the radio that measured the highest RSSI.
Detected By	The name and IP Address of the Connected RLX2 that detected the AP with the strongest RSSI.
First Detected	The date/time that the AP was first detected by any Connected RLX2. Only the time is shown if the date is the same as the current date.
Last Detected	The elapsed time since information was last received for the AP. Can occur if an AP is powered down or moved out of range.
Is ProSoft	Indicates **Yes** if the AP is a ProSoft Technology RLX2 radio, **No** otherwise.
RLX2 Name	The name of the radio if it is an RLX2. This column will only contain a value in the **Connected RLX2s** section.
WL Added	The time that an AP was added to the whitelist.

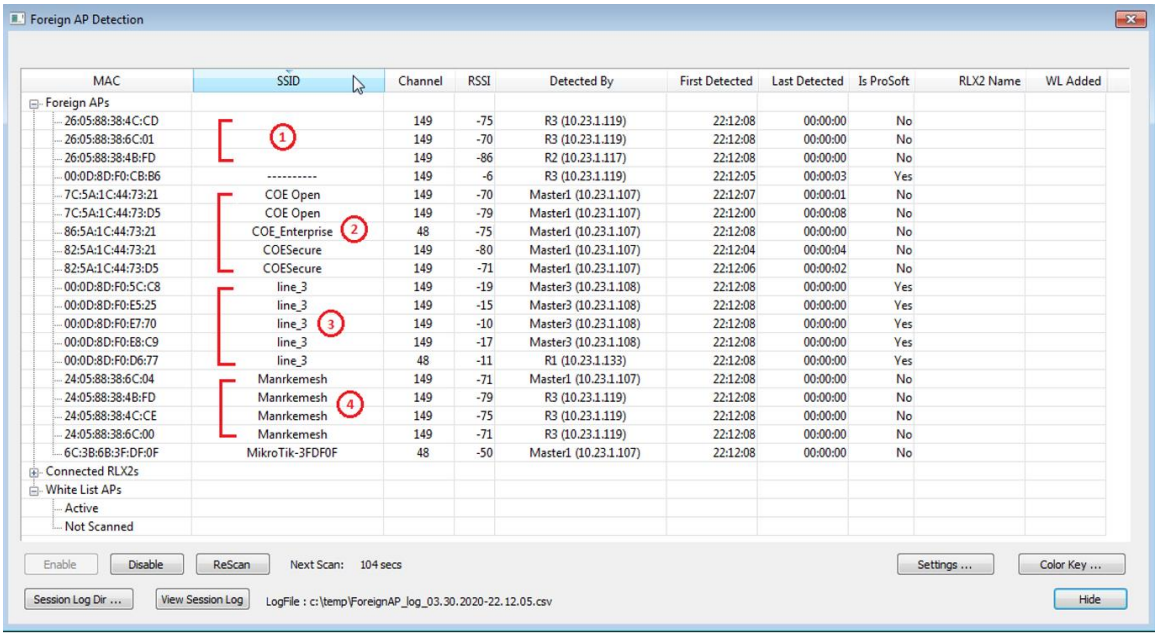
Right-clicking on any AP row in the view will present the following action menu. Only actions allowed or relevant are enabled with the others grayed out.



12.2 Adding APs to the Whitelist

The following SSID sorted list shows that there are 4 other systems on the channels of our network plus two single APs. In all cases the actions to take are as follows:

- If an AP or set of AP's belong to your organization and should be operating on the these channels, then they can be whitelisted.
- If an AP or set of AP's belong your organization but should not be operating on these channels, then your IT department should move them to a different channel.
- If an AP or set of AP's does not belong to your organization, then take steps to identify its location. If it's deemed legitimate (e.g. a neighbor's system) then whitelist, otherwise remove the AP.



In our example there are 6 sets of APs that have to be addressed.

1 This set of 3 APs has no SSID displayed which means the APs have 'hidden' their SSID. In this case the only identification that can be used to find these APs are their MAC addresses.

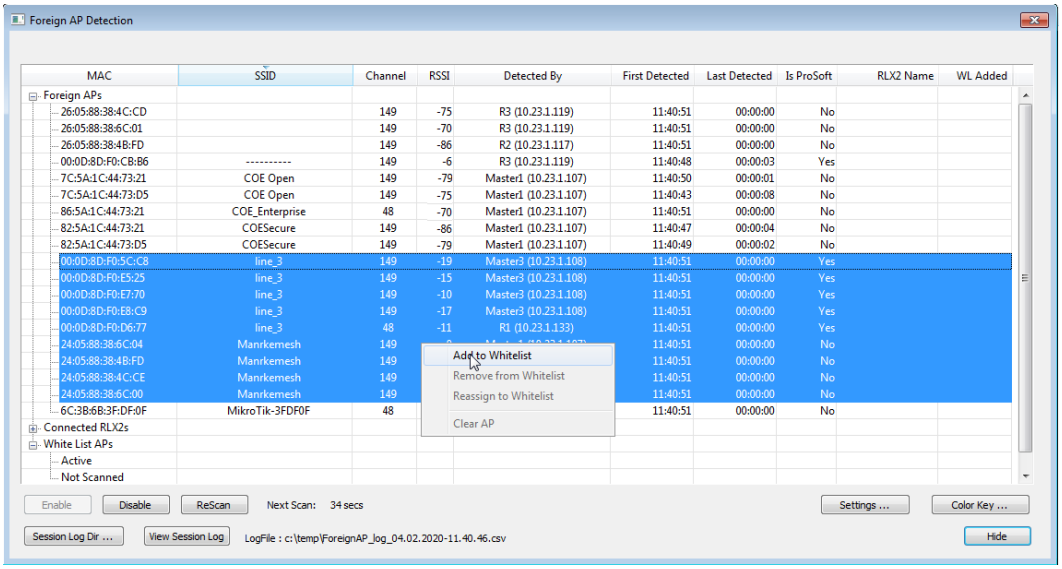
2 This "COE" system has 3 related SSIDs but have APs on both of our channels (48 and 149). Its RSSIs indicate that it is not very close to our system.

3 This "line_3" network is made up of ProSoft units. Since it did not appear in the list of "Connected RLX2s" it means that these units' Ethernet network is isolated from the Ethernet of line_1 and line_2 but within wireless range. In fact they are probably co-located as their RSSI is very strong.

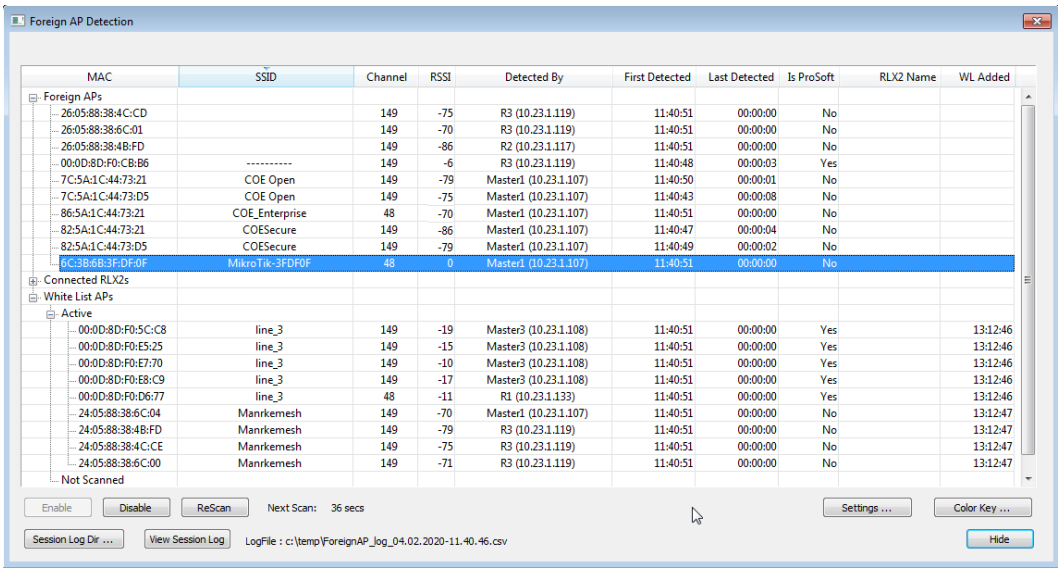
4 The "Manrkemesh" system has 4 APs on channel 149. Given its RSSIs are very low this system is also not close by.

The AP with SSID "---------" is an RLX2 unit in Repeater mode but configured to not allow other Repeaters to connect to it (*Allow Children* parameter set to **No**).

To add an AP to the whitelist right-click on the AP (or multiple AP's) and click on the **ADD TO WHITELIST** option.

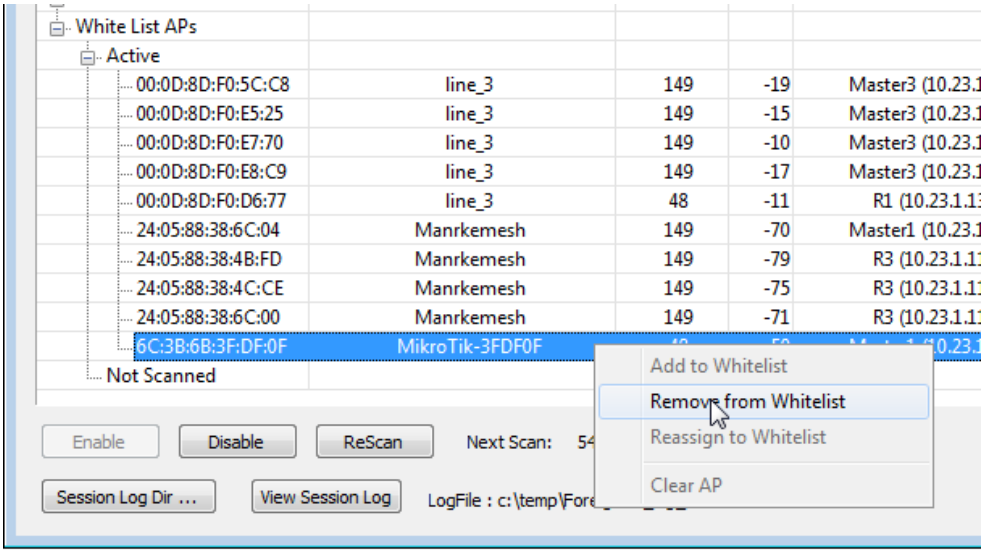


The selected APs now appear in the **White List APs** section as **Active** nodes. The *WL Added* column now shows the time that these APs were added to the whitelist.



12.3 Removing APs from the Whitelist

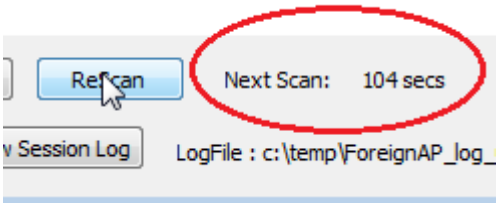
If an AP is mistakenly added to the whitelist it can be removed by right-clicking on the AP's row and selecting the **REMOVE FROM WHITELIST** option.



12.4 Forcing a Scan

The *Foreign AP Detection* window requests new scan data from the Connected radios every 120 seconds by default. This value can changed using the *Settings* dialog (for more information, see section *12.5 Foreign AP Detection Settings*.

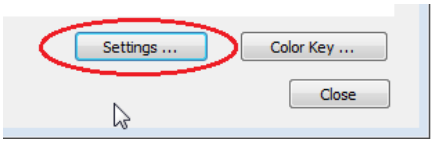
The time to the next scan event is shown in the display:

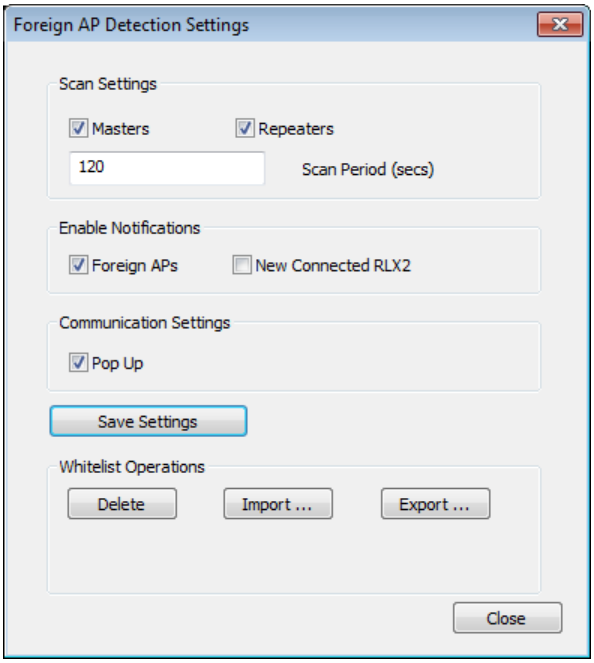


Clicking on the **RESCAN** button will initiate an immediate scan and the timer will reset to the scan interval value.

12.5 Foreign AP Detection Settings

Clicking on the **SETTINGS** button opens the *Foreign AP Detection Settings* dialog.

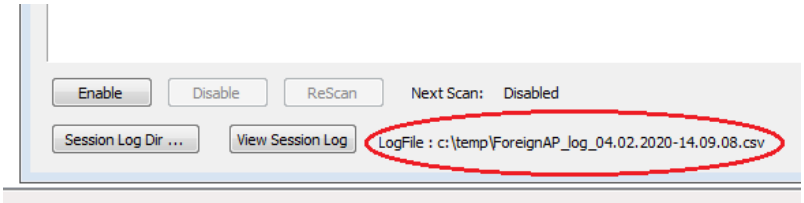




Scan Settings	**Description**
Masters	Uses all Connected Masters as a source of scan data.
Repeaters	Uses all Connected Repeaters as a source of scan data.
Scan Period	Sets the time interval at which the IH Browser queries enabled Masters and/or Repeaters for their scan information. Enter a value between **30** and **3600** seconds.
Enable Notifications	
Foreign APs	A notification is made when a new Foreign AP is detected.
New Connected RLX2	A notification is made when a new RLX2 is added to the **Connected RLX2s** section.
Communication Settings	
Pop Up	A pop-up is used as means of a notification. **Note:** At present this is the only communication mechanism for notification events.
Whitelist Operations	
Delete	Click to delete the current whitelist.
Import…	Click to import a whitelist file. **Note:** This will overwrite any whitelist currently being maintained by the Foreign AP Detection feature. First perform an export to save the current whitelist if you wish to retain the current whitelist for future use.
Export…	Click to export the whitelist to a file. This file can then be imported by any IH Browser that wishes to use this whitelist.
Save Settings	Saves any changes made to the settings in this dialog.

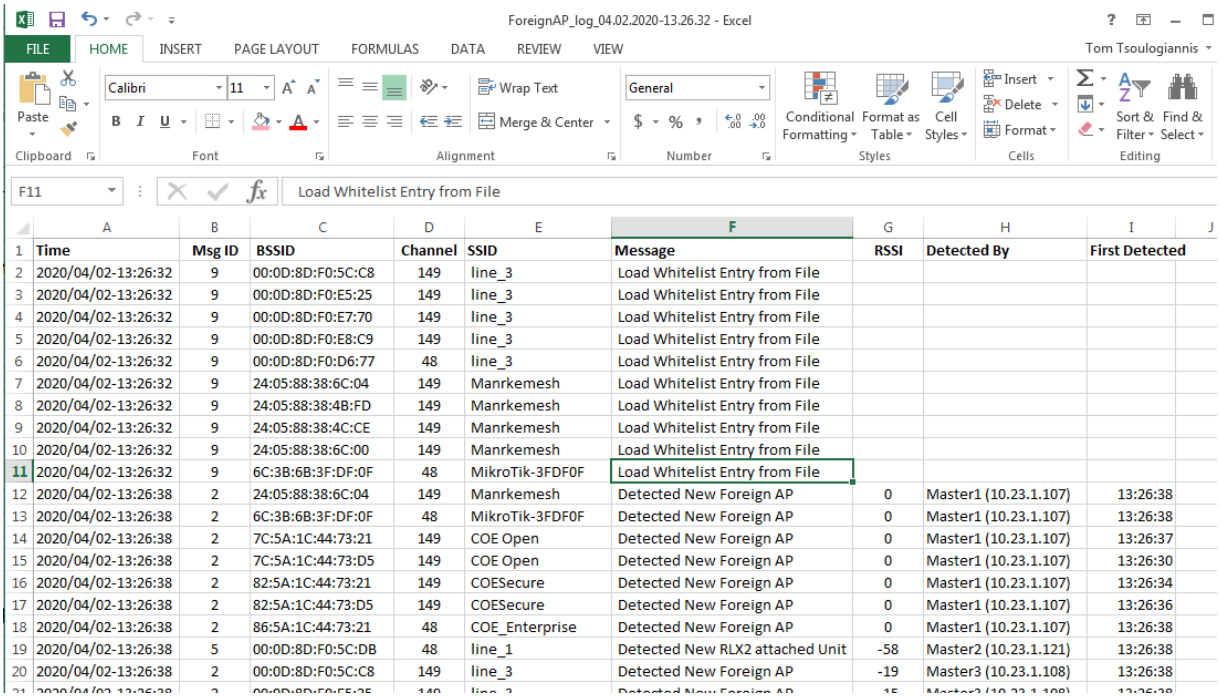
12.6 Session Log

The *Foreign AP Detection* window maintains a session log with information on each event that occurs such as detecting a new Foreign AP as well as moving APs from/to the whitelist.



The session log location is shown at the bottom of the *Foreign AP Detection* window. To change the directory the log is written to, click the **SESSION LOG DIR…** button.

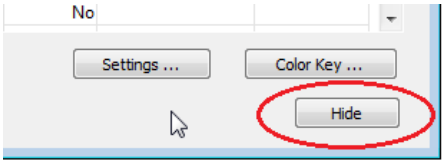
Each time Foreign AP Detection is enabled, a new session file is started in the directory. The session file is a CSV and can be opened by any spreadsheet program. The file name used includes the date and time the session file was started.



	A	B	C	D	E	F	G	H	I
1	Time	Msg ID	BSSID	Channel	SSID	Message	RSSI	Detected By	First Detected
2	2020/04/02-13:26:32	9	00:0D:8D:F0:5C:C8	149	line_3	Load Whitelist Entry from File			
3	2020/04/02-13:26:32	9	00:0D:8D:F0:E5:25	149	line_3	Load Whitelist Entry from File			
4	2020/04/02-13:26:32	9	00:0D:8D:F0:E7:70	149	line_3	Load Whitelist Entry from File			
5	2020/04/02-13:26:32	9	00:0D:8D:F0:E8:C9	149	line_3	Load Whitelist Entry from File			
6	2020/04/02-13:26:32	9	00:0D:8D:F0:D6:77	48	line_3	Load Whitelist Entry from File			
7	2020/04/02-13:26:32	9	24:05:88:38:6C:04	149	Manrkemesh	Load Whitelist Entry from File			
8	2020/04/02-13:26:32	9	24:05:88:38:4B:FD	149	Manrkemesh	Load Whitelist Entry from File			
9	2020/04/02-13:26:32	9	24:05:88:38:4C:CE	149	Manrkemesh	Load Whitelist Entry from File			
10	2020/04/02-13:26:32	9	24:05:88:38:6C:00	149	Manrkemesh	Load Whitelist Entry from File			
11	2020/04/02-13:26:32	9	6C:3B:6B:3F:DF:0F	48	MikroTik-3FDF0F	Load Whitelist Entry from File			
12	2020/04/02-13:26:38	2	24:05:88:38:6C:04	149	Manrkemesh	Detected New Foreign AP	0	Master1 (10.23.1.107)	13:26:38
13	2020/04/02-13:26:38	2	6C:3B:6B:3F:DF:0F	48	MikroTik-3FDF0F	Detected New Foreign AP	0	Master1 (10.23.1.107)	13:26:38
14	2020/04/02-13:26:38	2	7C:5A:1C:44:73:21	149	COE Open	Detected New Foreign AP	0	Master1 (10.23.1.107)	13:26:37
15	2020/04/02-13:26:38	2	7C:5A:1C:44:73:D5	149	COE Open	Detected New Foreign AP	0	Master1 (10.23.1.107)	13:26:30
16	2020/04/02-13:26:38	2	82:5A:1C:44:73:21	149	COESecure	Detected New Foreign AP	0	Master1 (10.23.1.107)	13:26:34
17	2020/04/02-13:26:38	2	82:5A:1C:44:73:D5	149	COESecure	Detected New Foreign AP	0	Master1 (10.23.1.107)	13:26:36
18	2020/04/02-13:26:38	2	86:5A:1C:44:73:21	48	COE_Enterprise	Detected New Foreign AP	0	Master1 (10.23.1.107)	13:26:38
19	2020/04/02-13:26:38	5	00:0D:8D:F0:5C:DB	48	line_1	Detected New RLX2 attached Unit	-58	Master2 (10.23.1.121)	13:26:38
20	2020/04/02-13:26:38	2	00:0D:8D:F0:5C:C8	149	line_3	Detected New Foreign AP	-19	Master3 (10.23.1.108)	13:26:38

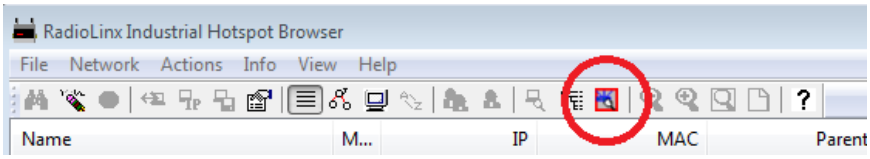
12.7 Hiding the Foreign AP Detection window

When the Foreign AP Detection feature is active, the button at the bottom right of the window changed from **CLOSE** to **HIDE**. Note that the IH Browser cannot be closed if the feature is running. Clicking on the **HIDE** button closes the window but the feature remains active.



The current status of the Foreign AP Detection function can always be viewed from the IH Browser's Toolbar. When the feature is active, the Foreign AP Detection icon is green.

If a Foreign AP is detected while the window is closed, the icon turns red.



13 Device Management

This feature allows for the detection and commissioning of new RLX2/ELXM series radios that are added to the network. An un-commissioned radio is one that has been reset to its Default state.

In addition, it continually monitors operational wireless radios to determine if they are compliant to network administrator rules configured into this feature.

The following are the key capabilities of the *Device Management* feature:

- Uses a CSV file prepared by the network administrator to specify how the radio should be configured.
- Identify un-commissioned RLX2 or ELXM radios.
- Commission the radio with the correct operating firmware and configuration.
- Monitor operational radios whose configuration is non-compliant.
- The following are checked against the content of the CSV file:
  - The radio Name
  - The configuration image signature
  - The firmware image version
  - The User Default configuration image signature
  - For radios in AP mode, the channel number and transmit power
  - DHCP is enabled or, the configured IP Address.

13.1 CSV File

Device Management is accomplished using a CSV file that contains the list of RLX2/ELXM series radios to be managed. Columns in the CSV file define settings to be used for each radio. The *Device Management* feature is enabled as soon as a CSV file is loaded. Removal of the CSV file disables the *Device Management* feature.

When a CSV file is loaded it will be internally saved. Subsequent changes to the CSV file will not have any effect. To adopt the changes the CSV file must be reloaded.

The CSV file will be **validated and checked** for errors when it is loaded.

- Firmware or Configuration files referenced in the CSV will be accessed to ensure they are present.
- Version or Signature information will be extracted from the files and stored.
- Ensure that the **Mode** field is specified in each row and verify that the Operating Configuration image in the row matches the specified Mode.
- Any error in a row will prevent the updating of a radio that matches the row until the row is corrected.
- A notification is made in the *Device Management* dialog's *Show CSV File Entries* list view **Notes** column.
- Column order does not matter and all columns do not need to be present. The Column Name in the 1st row indicates the field in the column.

The following examples show a partial view of the CSV file columns as they appear when opened in a spreadsheet program.

Note: This CSV file is loaded into the IH Browser from *Device Management* dialog. Once loaded it is active.

13.1.1 Spreadsheet View

MacAddr	UnitName	SSID	Mode	IPAddr	UsingDCHP	Operation	ConfigFile	FWFile
*	agv	Net1	Client		true	Both	C:\Net1.cfg	C:\RLX2_v040A_R
00.0D.8D.F0.5C.C9	SC-AP4		AP		true	Monitor	C:\Net1.cfg	C:\RLX2_v040A_R
000D8DF07919	SC-AP3		AP		true	Monitor	C:\Net1.cfg	C:\RLX2_v040A_R
00:0D:8D:F0:E8:C4	SC-AP2		AP		true	Monitor	C:\Net1.cfg	C:\RLX2_v040A_R
00.0D.8D.AA.03.CD	SC-AP1		AP	192.168.1.2	false	Commission	C:\Net1.cfg	C:\RLX2_v040A_R

13.1.2 Text Editor View

```
MacAddr, UnitName, SSID, Mode, IPAddr, UsingDHCP, Operation, ConfigFile, FWFile
*, agv,Net1, , AP, , true, Both, C:\Net1.cfg, C:\RLX2_v0040A_R
00.0D.8D.F0.5C.C9, SC-AP4, , AP, , true, Monitor, C:\Net1.cfg, C:\RLX2_v0040A_R
000D8DF07919, SC-AP3, , AP, , true, Monitor, C:\Net1.cfg, C:\RLX2_v0040A_R
00:0D:8D:F0:E8:C4, SC-AP2, , AP, , true, Monitor, C:\Net1.cfg, C:\RLX2_v0040A_R
00.0D.8D.AA.03.CD, SC-AP1, , AP, 192.168.1.2, false, Commission, C:\Net1.cfg, C:\RLX2_v0040A_R
```

13.1.3 CSV Column Description

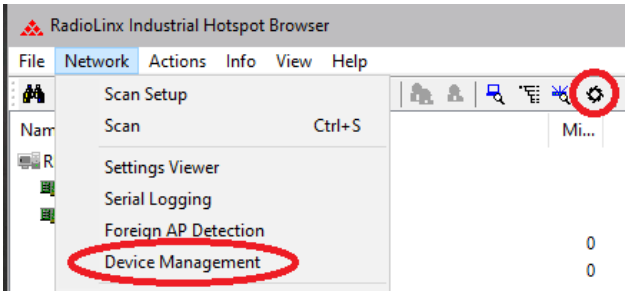
Column/Field Name	Values	Description/Use
MacAddr	xx.xx.xx.xx.xx.xx or '*'	The MAC address of the radio to be monitored or commissioned. A wildcard char '*' can be specified instead to match all mac addresses. The Address is in hexadecimal byte format with a '.' or ':' delimiter between bytes.
UnitName	string	This is the name assigned to the radio. How this field is used when a radio matches a CSV file row depends on what update action is being taken. Up to 32 characters and can be upper- or lower-case letters, numbers, '-', '_' or blanks. If updating the User Defaults Configuration of a radio, this field is ignored and the name in the configuration will be used. If updating an Operational Configuration: • If Name is blank, then preserve unit's current name during the update. • If Name is present, set this Name during the update. If the *Operation* column is set to **Monitor**: • And this field is not blank • And the matching radio's name is different Then update the radio so it uses this Name.

SSID	string	This field is informational and is not used in either matching or monitoring unless the *MacAddr* field is the wildcard *.
Mode	AP/Client	The mode for this CSV entry. It must be specified on each line. The configuration file specified must be for the specified mode. If the *Operation* column is set to **Monitor**, only radios that match this mode field will be updated. i.e. the *Device Management Monitoring* feature cannot be used to change the operating mode of the radio. To do so would require the radio to be reset to defaults then re-commissioned with the new mode.
IPAddr	ddd.ddd.ddd.ddd	If DHCP is not set, then this IP address will be set into the matching radio.
UsingDCHP	true/false	The DHCP mode - If set to **true**, any configuration update will force the radio to enable DHCP.
Operation	Monitor/Commission/ Both	This value must be set on each line in the CSV. It will govern the operation of that line. **Monitor**: Operational radios that match the *MacAddr* and *Mode* fields in this CSV row will be monitored for field values that differ (*Unit Name*, *F/W version*). Radios with values that differ will be listed in the *Device Management* dialog's *Units Requiring Updating List View*. **Commission**: Un-commissioned radios that match the *MacAddr* and *SSID* fields will be commissioned with the field values in this CSV row. (FWFile) **Both**: The information will be used for both Commissioning and Monitoring. Action taken will depend on whether the radio is un-commissioned or operational.
ConfigFile	string - filename with full path	The full path to a configuration file that is used when updating either un-commissioned or operational radios. The signature in this file is compared against the Configuration signature currently in radio. Only if the signatures are different will the configuration file be included when updating a radio.
FWFile	string - filename with full path	The full path to a firmware file. The f/w version in **Monitored** radios will be compared against the f/w version in this file. Only if the versions are different will the firmware be included when updating a radio.
Channel	int	When managing a channel plan for a set of Access Points, this parameter can be used to specify the channel the AP should use. A Monitored AP's advertised channel being different than this value will trigger an update. This value will be set into the radio on any update if the *Mode* is **AP**. This field is ignored if the *Mode* is **Client**.
TxPower	int	On CSV lines where the *Mode* is **AP** this field sets the radio's transmit power level. A Monitored AP's advertised transmit power level being different than this value will trigger an update. This value will be set into the radio on any update if the *Mode* is **AP**. This field is ignored if the *Mode* is **Client** or blank.

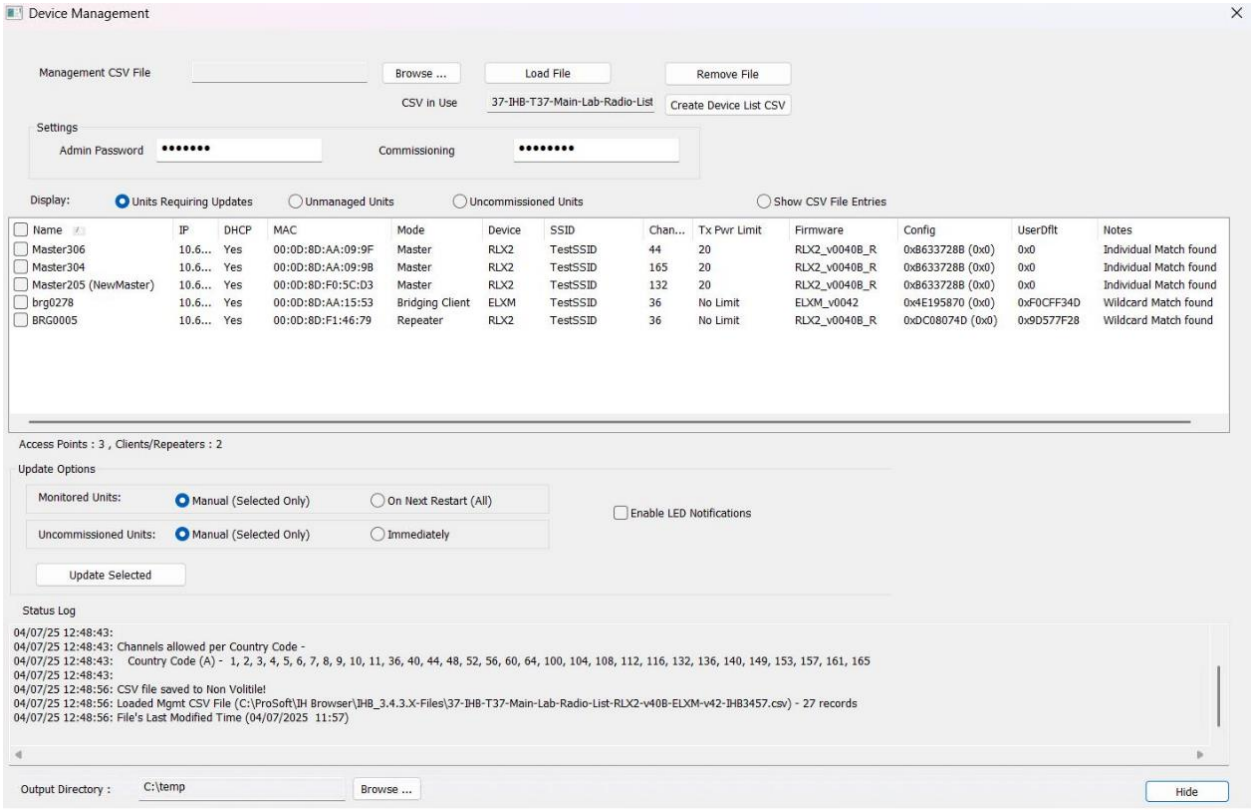
		A value of **0** means the radio will use the max power it is capable of on any channel. Valid values are **10** to **29** dBm.
CommissionSSID	String	When an un-commissioned radio is detected the MAC Address and this SSID must match to trigger updates to commission the radio.
UserDfltFile	string - filename with full path	If it is desired to reset a radio to a known state different from the radio's Factory Defaults, the radio can be loaded with a special configuration known as "*User Defaults*" in addition to the existing "*Factory Defaults*". When the radio is reset to *User Defaults* it will load the saved User Default configuration. Only if the radio's User Defaults signature is different from that in the *UserDfltFile* will the User Default file be included when updating a radio.
UserDfltFlags	int - bitmask 0x01 - Set Uncommissioned 0x02 - Name Detect	These are additional flags that can be set along with the *User Defaults* config file. **Set Un-commissioned**: When the radio is reset to its User Defaults, it will cause the radio to advertise itself as *un-commissioned*. This option is only valid when in **Client** mode. **Name Detect:** This will enable learning a number to add to the end of the *UnitName* by inspecting the radio names in DHCP Requests sent by devices on the radio's Ethernet and extracting any trailing numbers. This option is only valid when in **Client** mode.

13.2 The Device Management Dialog

The *Device Management* dialog can be opened by clicking on **NETWORK** > **DEVICE MANAGEMENT**, or by clicking the **DEVICE MANAGEMENT** icon in the shortcuts bar.



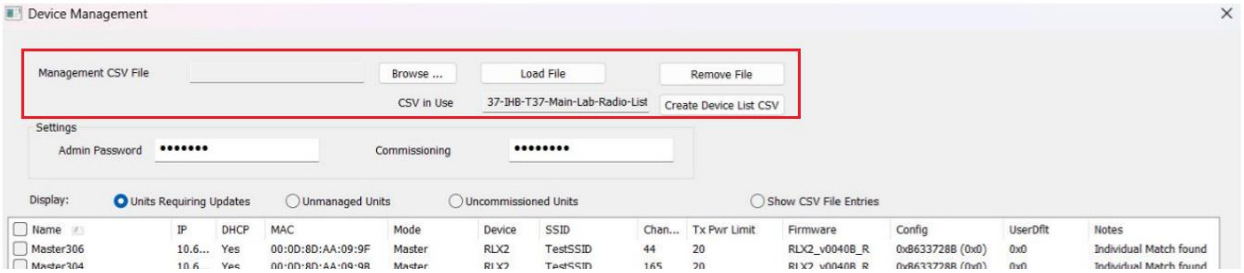
When the menu item or the Icon is selected the *Device Management* dialog will appear.



The **DEVICE MANAGEMENT** icon background color will give an indication of the current state of the feature.

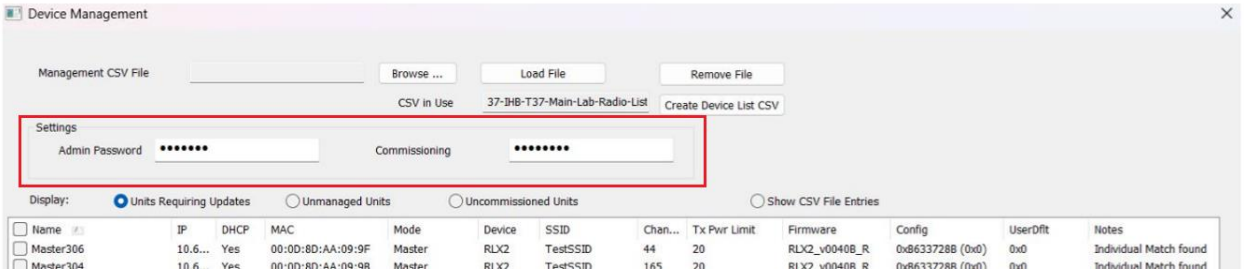
Icon Background Color	State
None	Feature is disabled.
Green	Feature is set to automatically update radios.
Red	The CSV file has errors in it.
Yellow	The feature is in manual mode and radios require updates.

13.2.1 Device Management CSV Controls



Parameter	Description
Management CSV File	The CSV file to be used to manage the radios. The CSV file contains a row per radio to be managed, identified by the MAC Address, and has columns specifying the files and settings for the radio. **Note:** For Client radios that are identically configured, a single row can be used with an * wildcard in the *MacAddr* column.
Browse	Browse and select the CSV file to be used.
Load File	To activate a new CSV file that has been selected, click the **LOAD FILE** button. **Note:** The *Device Management* feature is automatically enabled once a CSV file is loaded.
Remove File	Removes the CSV file. **Note:** The *Device Management* feature can only be disabled by removing the CSV file.
CSV in use	Informative display showing the current CSV file name in use.
Create Device List CSV	Creates a CSV device list for all radio Access Points currently detected. **Note:** Each managed Access Point would require its own row in the CSV file.

13.2.2 Device Management Common Settings



Parameter	Description
Admin Password	The password in use by the RLX2/ELXM series radios. This will be used when updating firmware and configuration.
Commissioning Password	The password to use when an un-commissioned radio is detected. An un-commissioned radio is running either Factory or User Defaults and as such its password is different than an operational radio.

13.2.3 Device Management List View Display

A list view window in the *Device Management* dialog displays lists of radios under various categories. A set of radio buttons allows the selection of the category.

There is a column in the list for each parameter used or managed by the CSV file. A mismatch is shown by displaying the CSV value of the parameter followed by the current value in use in brackets.

e.g. 36 (165) for Channel
14 (No Limit) for Tx Power Limit

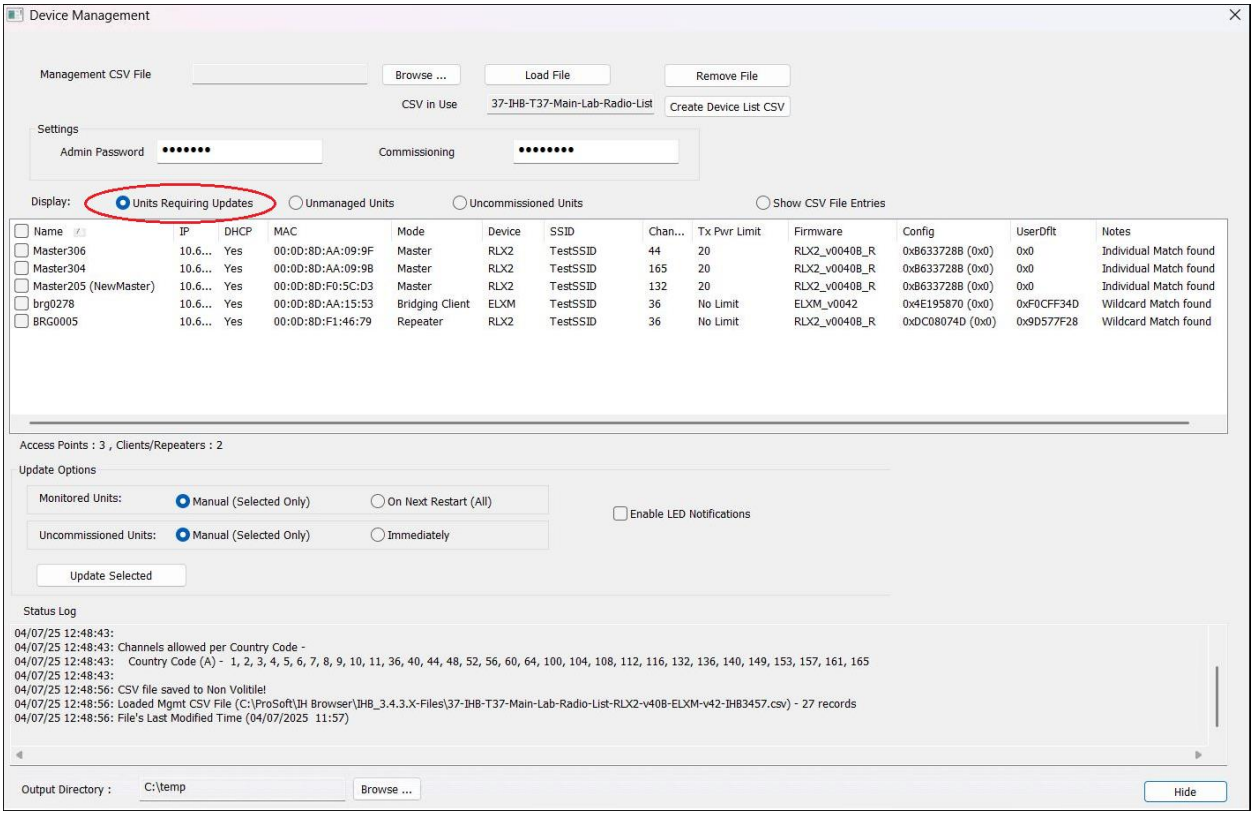
A *Notes* column identifies exception conditions that were encountered with the radio.

At the beginning of each row a Check Box is present to allow the user to select one or more radios when performing manual updates.

The checkbox next to the *Name* label can be used to select or deselect all radios in the list.

13.2.3.1 Units Requiring Updates

When the **UNITS REQUIRING UPDATES** radio button is selected the list will display radios whose current state differs from its matching entry in the CSV file.

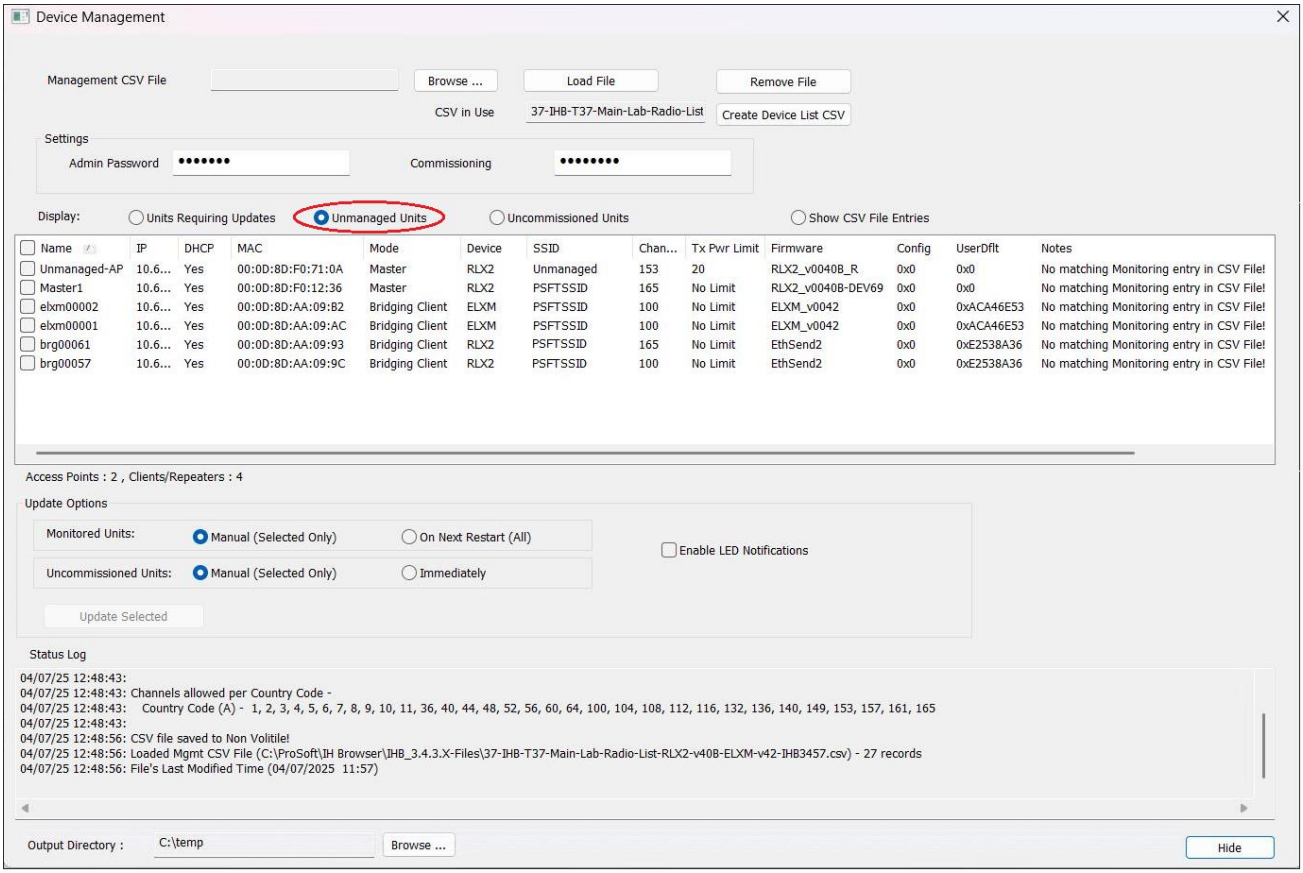


Fields that do not match are indicated by the desired value followed by the value currently in use on the radio in brackets as shown above in the *Config* column.

13.2.3.2 Unmanaged Units

When the **UNMANAGED UNITS** radio button is selected the list will display any devices discovered on the network for which there was no match in the CSV file. This is also stated in the *Notes* column.

If these radios were unintentionally left out of the CSV file, the user needs to edit the CSV file to add these radios and then re-load it in the *Device Management* dialog. Once reloaded the listed unmanaged radios should disappear once they are re-discovered.

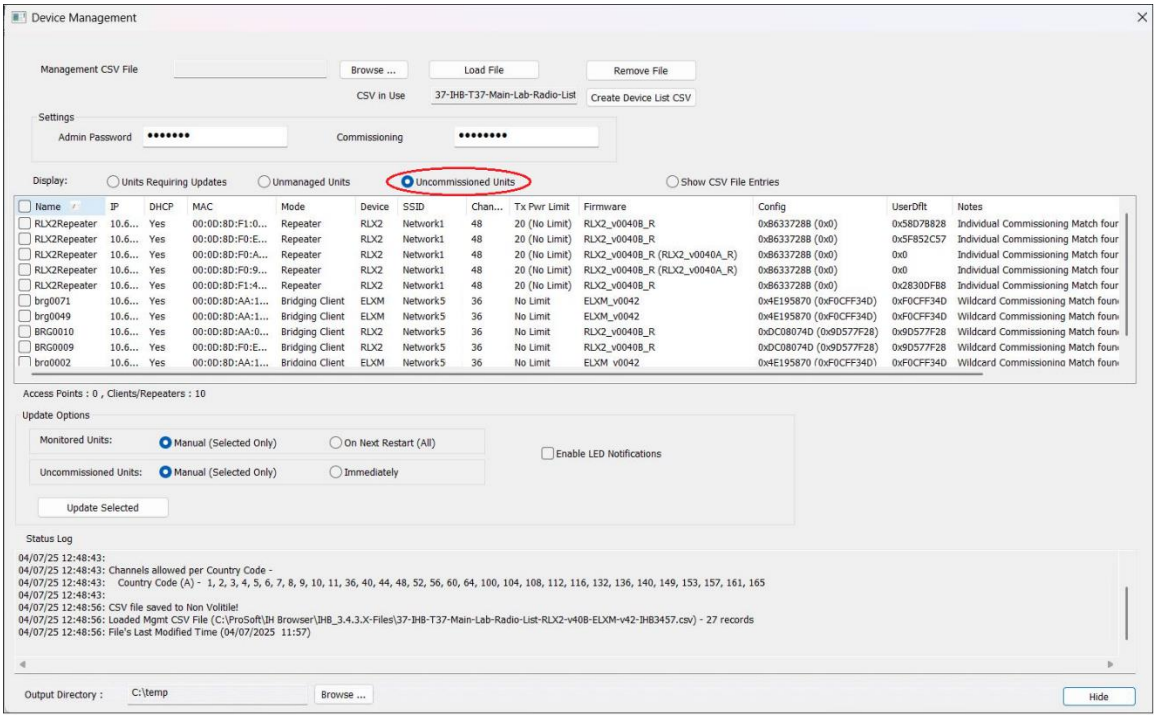


13.2.3.3 Uncommissioned Units

When the **UNCOMMISSIONED UNITS** radio button is selected the list will display radios discovered on the network that are currently in an un-commissioned state and an entry in the CSV file matches the radio's MAC Address and SSID.

The current values in the radio are in brackets where they differ from the value specified in the CSV for the matching row, indicating what will be updated during the commissioning process.

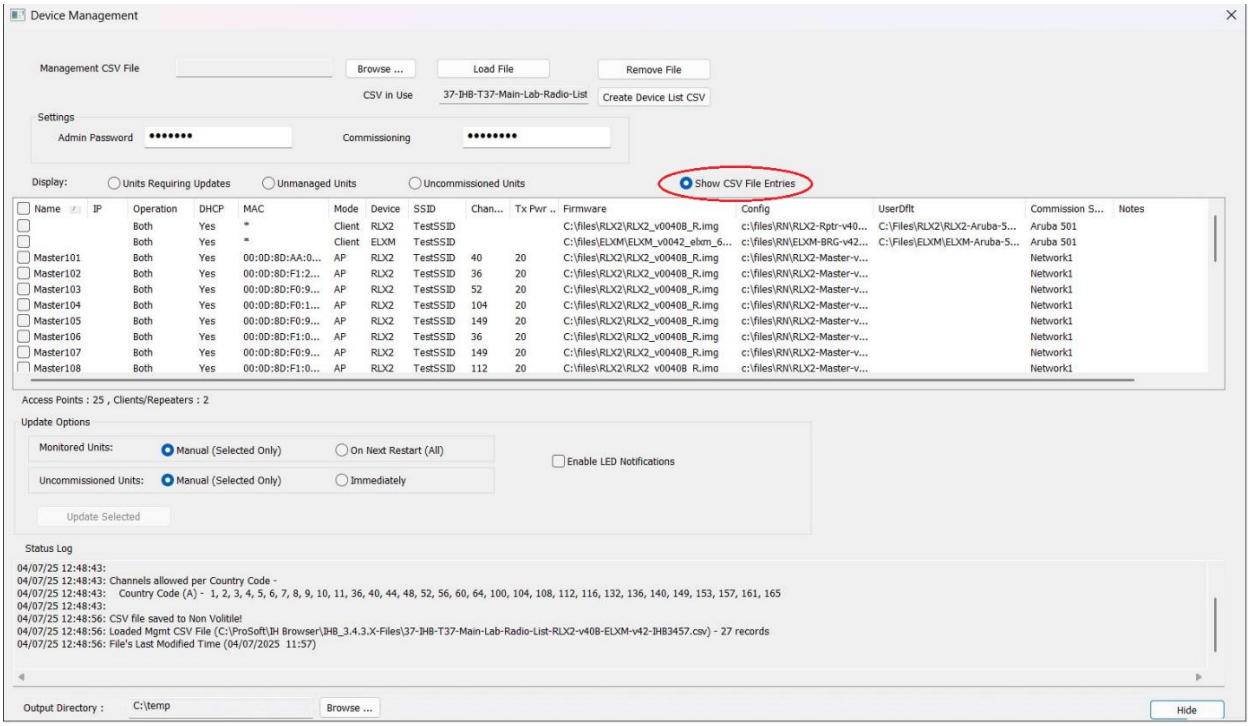
Once commissioned the radio will disappear once it is re-discovered and is in its operational state.



13.2.3.4 Show CSV File Entries

When the **SHOW CSV FILE ENTRIES** radio button is selected, the list will display the entries that were loaded from the CSV file. This allows a quick way to review what was in the CSV file.

The cells that were blank in the CSV file will also be blank in this list view.



13.2.4 Update Options

This section of the *Device Management* dialog separately configures how updates are handled for Monitored and Un-commissioned radios.

Update Options	Description
Monitored Units	**MANUAL** (selected only) Updates will only be done manually on monitored radios that appear in the *Units Requiring Updates* list. The user selects the radios to update in that list and then clicks the **UPDATE SELECTED** button to initiate the updates. **ON NEXT RESTART** (All) This option will trigger an automatic update on any radio in the *Units Requiring Updates* list as soon as the *Device Management* function detects that the radio has restarted. This detection must occur within 2 minutes of the radio restarting. This 2-minute window is implemented primarily for updating the radio in a mobile platform on the premise that the platform itself also rebooted and was in a safe location. After 2 minutes there is a high probability that the platform has been put into service.
Un-commissioned Units	**MANUAL** (selected only) Commissioning will only be done manually on radios that appear in the *Un-commissioned Units* list. The user selects the radios to commission in that list and then clicks the **UPDATE SELECTED** button to initiate the commissioning sequence. **IMMEDIATELY** Automatically commissions any radio added to the *Un-commissioned Units* list. There is no uptime restriction on starting the commissioning sequence.
Enable LED Notifications	This parameter will send an LED pattern notification to a radio that is in either the *Un-commissioned Units* or *Unmanaged Units* list to flash its LEDs in a distinct pattern depending on which list it is on. This allows visual indication that a radio is not yet in an operational state, and if it persists some action may need to be taken by a technician.
Status Log	Information on the progress of updates and other events is displayed in this window for informational purposes.

13.3 Device Management Operation

A brief description of the operating modes and rules of the *Device Management* feature as related to the CSV file content.

13.3.1 Commissioning Rules

The CSV rows that have the *Operation* field set to **Commission** or to **Both** will be considered when searching the CSV list for a match for a detected un-commissioned radio. To match a row an un-commissioned radio's MAC Address and SSID must be the same as these respective fields in that row.

It is possible to set the *MacAddr* field in the CSV to the Wildcard '*' which will then match to any radio, in which case if the SSID configured into the un-commissioned radio is the same as the *CommissionSSID* field string then a match is declared.

The search through the CSV will first ensure that a radio's MAC address does not appear in any row before a wildcard row is considered.

Once a match is made to a CSV row, the un-commissioned radio is added to the *Un-commissioned Units List* view in the *Device Management* dialog and if the *Update Options* have been set to **IMMEDIATELY** an update of the radio starts right away based on the settings and files set into fields in the row.

If the *Update Options* for commissioning are set to **MANUAL**, then the user must select the radio from the *Uncommissioned Units* list and click the **UPDATE SELECTED** button to initiate the update.

13.3.2 Monitoring Rules

Rows that have the *Operation* field set to **MONITOR** or **BOTH** will be considered when searching the CSV file to match to a radio that is already commissioned.

To declare a match to a CSV row, the *Mac Address*, *Mode*, and *SSID* fields must be the same as the current state of the radio.

If a MAC Address is specified, then that MAC Address must only appear in the CSV file once.

The *MacAddr* field takes precedence. When populated, a radio matching that MAC Address will only be assessed based on that row of the CSV file and not a wildcard row.

If the radio's MAC address is not found in the CSV file, then the search reverts to looking for the 1st matching wildcard row.

The 1st row encountered in the CSV file that has an * in the MAC Address cell, and the *Mode* and the *SSID* fields match the radio's current state, then this row will be used.

If no match for a radio is found in the CSV file then this radio will appear in the *Unmanaged Units* list in the *Device Management* dialog. This list can be reviewed, and the CSV file updated if these radios need to be managed.

Radios that match a CSV row but differ in firmware version or settings with one or more fields of the CSV row are added to the *Units Requiring Updates* list in the *Device Management* dialog. The action taken by the IH Browser will depend on the state of the *Monitored Units* control in the *Update Options* section of the *Device Management* dialog.

Updates for the radio can be configured to be done manually by the user, or they can be triggered when the IH Browser detects the radio has restarted.

Once a radio is up to date it is no longer visible in the *Device Management* dialog.

14 Support, Service, and Warranty

14.1 Contacting Technical Support

ProSoft Technology, Inc. is committed to providing the most efficient and effective support possible. Before calling, please gather the following information to assist in expediting this process:

1. Product Version Number
2. System architecture
3. Network details

If the issue is hardware related, we will also need information regarding:

1. Module configuration and associated ladder files, if any
2. Module operation and any unusual behavior
3. Configuration/Debug status information
4. LED patterns
5. Details about the interfaced serial, Ethernet or Fieldbus devices

North America (Corporate Location)	**Europe / Middle East / Africa Regional Office**
Phone: +1 661-716-5100 ps.prosofttechnology@belden.com Languages spoken: English, Spanish REGIONAL TECH SUPPORT ps.support@belden.com	Phone: +33.(0)5.34.36.87.20 ps.europe@belden.com Languages spoken: English, French, Hindi, Italian REGIONAL TECH SUPPORT ps.support.emea@belden.com
Latin America Regional Office	**Asia Pacific Regional Office**
Phone: +52.222.264.1814 ps.latinam@belden.com Languages spoken: English, Spanish, Portuguese REGIONAL TECH SUPPORT ps.support.la@belden.com	Phone: +60.3.2247.1898 ps.asiapc@belden.com Languages spoken: Bahasa, Chinese, English, Hindi, Japanese, Korean, Malay REGIONAL TECH SUPPORT ps.support.ap@belden.com

For additional ProSoft Technology contacts in your area, please visit:
www.prosoft-technology.com/About-Us/Contact-Us

14.2 Warranty Information

For complete details regarding ProSoft Technology's legal terms and conditions, please see:
www.prosoft-technology.com/ProSoft-Technology-Legal-Terms-and-Conditions

For Return Material Authorization information, please see:
www.prosoft-technology.com/RMA