ProSoft TECHNOLOGY

Where Automation Connects.

ELXM-SW6

ProLinx Edge™ Mini

802.11a, b, g, n, ac, ax

May 8, 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

ELXM-SW6 User Manual
For Public Use.

May 8, 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

Important Safety Information

The following Information and warnings pertaining to the radio module must be heeded:

WARNING – EXPLOSION HAZARD – DO NOT REPLACE ANTENNAS UNLESS POWER HAS BEEN SWITCHED OFF OR THE AREA IS KNOWN TO BE NON-HAZARDOUS.

"THIS DEVICE CONTAINS ONE OF THE FOLLOWING TRANSMITTER MODULES:
FCC ID: 2AE3B-ACB-QCA206X
PLEASE SEE FCC ID LABEL ON THE SIDE OF THE DEVICE."

"THIS DEVICE USES AN INTERNAL COMPACT FLASH RADIO MODULE AS THE PRIMARY RADIO COMPONENT. THE COMPACT FLASH RADIO MODULE DOES NOT HAVE AN FCC ID LABEL. THE COMPACT FLASH RADIO MODULE HAS NO USER SERVICEABLE PARTS."

"THIS DEVICE COMPLIES WITH PART 15 OF THE FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS: (1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE, AND (2) THIS DEVICE MUST ACCEPT ANY INTERFERENCE RECEIVED, INCLUDING INTERFERENCE THAT MAY CAUSE UNDESIRED OPERATION."

"CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE COULD VOID THE USER's AUTHORITY TO OPERATE THE EQUIPMENT."

"This device is configured for operation in the USA during manufacturing. These configuration controls are not present in the software with which the unit is shipped; therefore, the end user cannot change the max power settings or the country/region. The models sold & shipped within the U.S. are identified within the model number with –A as part of the identifier."

China RoHS Hazardous Material Declaration Table

部件名称 Component Name	有害物质 Hazardous Substances					
	鉛 Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六价铬 Hexavalent Chromium (Cr(VI))	多溴联苯 Polybrominated Biphenyls (PBB)	多溴二苯醚 Polybrominated Diphenyl Ethers (PBDE)
印刷电路板组件 Printed Circuit Board Assemblies	X	O	O	O	O	O
金属部件 Metal Components	X	O	O	O	O	O
电池 Battery	O	O	O	O	O	O

本表格依据SJ/T 11364的规定编制。This table is made per guidance of SJ/T 11364

O: 表示该有害物质在该部件所有均质材料中的含量均在GB/T 26572规定的限量要求以下。

O: Indicates that this hazardous substance contained in all of the homogeneous materials for the part is below the limit requirement in GB/T 26572.

X: 表示该有害物质至少在该部件的某一均质材料中的含量超出GB/T 26572规定的限量要求。

X: Indicates that this hazardous substance contained in at least one of the homogeneous materials used for this part is above the limit requirement in GB/T 26572.

WARNING – EXPLOSION HAZARD – SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASSI, DIV.2

WARNING – EXPLOSION HAZARD – WHEN IN HAZARDOUS LOCATIONS, TURN OFF POWER BEFRE REPLACING OR WIRING MODULES

WARNING – EXPLOSION HAZARD – DO NOT DISCONNECT EQUIPMENT UNLESS POWER HAS BEEN SWITCHED OFF OR THE AREA IS KNOWN TO BE NON-HAZARDOUS

Industry Canada Requirements:

"THIS DEVICE HAS BEEN DESIGNED TO OPERATE WITH AN ANTENNA HAVING A MAXIMUM GAIN OF 24 dB. AN ANTENNA HAVING A HIGHER GAIN IS STRICTLY PROHIBITED PER REGULATIONS OF INDUSTRY CANADA. THE REQUIRED ANTENNA IMPEDANCE IS 50 OHMS."

"TO REDUCE POTENTIAL RADIO INTERFERENCE TO OTHER USERS, THE ANTENNA TYPE AND ITS GAIN SHOULD BE CHOSEN SUCH THAT THE EQUIVALENT ISOTROPICALLY RADIATED POWER (EIRP) IS NOT MORE THAN THAT REQUIRED FOR SUCCESSFUL COMMUNICATION."

"THE INSTALLER OF THIS RADIO EQUIPMENT MUST ENSURE THAT THE ANTENNA IS LOCATED OR POINTED SUCH THAT IT DOES NOT EMIT RF FIELD IN EXCESS OF HEALTH CANADA LIMITS FOR THE GENERAL POPULATION; CONSULT SAFETY CODE 6, OBTAINABLE FROM HEALTH CANADA."

Agency Approvals and Certifications

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

ELXM-SW6

This equipment is Suitable For Use in Class I, Division2, Groups A, B, C, D or Non-Hazardous Location Only.

WARNING – EXPLOSION HAZARD – Substitution of Any Components May Impair Suitability for Class I, Division 2.

WARNING – EXPLOSION HAZARD – Do not disconnect equipment unless power has been removed or the area is known to be non-hazardous.

WARNING – EXPLOSION HAZARD – The SIM Card/Personality Module connection is for initial setup and maintenance only. Do not use, connect, or disconnect unless area is known to be non-hazardous. Connection or disconnection in an explosive atmosphere could result in explosion.

Class 2 Power

Device is an open-type and is to be installed in an enclosure suitable for the environment.

Antenna Spacing Requirements for User Safety

It is important to keep the radio's antenna a safe distance from the user. To meet the requirements of FCC part 2.1091 for radio frequency radiation exposure, this radio must be used in such a way as to guarantee at least 20 cm between the antenna and users. Greater distances are required for high-gain antennas. The FCC requires a minimum distance of 1 mW *cm^2 power density from the user (or 20 cm, whichever is greater).

Note: If a specific application requires proximity of less than 20 cm, the application must be approved through the FCC for compliance to part 2.1093.

Table of Contents

1 Start Here

For most applications, the installation and configuration steps described in the following topics work without additional programming. ProSoft Technology strongly recommends completing the steps in this chapter before developing a custom application.

1.1 About This Document

This document covers the ProLinx Edge™ Mini ELXM-SW6 radio product.

Model	Standards	Maximum Output Power
ELXM-SW6	IEEE 802.11a/b/g/n/ac/ax	17 dBm (50 mW) per antenna

Note: The ELXM-SW6 is compatible with ProSoft Technology's RLX2 series of radios.

1.2 About the ELXM-SW6

1.2.1 Product Overview

The ELXM-SW6 is an industrial high-speed Ethernet radio. Use it in place of Ethernet cables to save money, extend range, or when communication with a moving platform is required. The ELXM-SW6 operates as a wireless Ethernet switch when the peer is another ProSoft Technology radio. This allows all layer 2 Ethernet data to be bridged between the radios.

The ELXM-SW6 can also connect to 3rd party Access Points (APs) and allows bridging of all IP based Ethernet traffic between the ELXM-SW6 and AP Ethernets.

The ELXM-SW6 is certified for unlicensed operation in the United States, Canada, Europe and other approved countries in the 2.4 and 5 GHz bands. Contact ProSoft Technology for a list of currently approved antennas.

A highly reliable wireless network can be developed by creating redundant wireless paths. Multiple Access Points (APs), either from ProSoft Technology or a 3rd party vendor, can be installed to form a wireless 802.11 Infrastructure. The ELXM-SW6 can connect to any AP at any time; if one AP goes down or is out of range, the ELXM-SW6 connects to another.

Note: Wi-Fi is a trademark of the Wi-Fi Alliance, used to describe the underlying technology of wireless local area networks (WLAN) based on the IEEE 802.11 specifications.

A high level of security is inherent with AES (Advanced Encryption Standard) encryption. TKIP (Temporal Key Integrity Protocol) is also available for backward compatibility but is not recommended as it is less secure. WEP128 or WEP64 (Wired Equivalent Protocol) encryption is no longer available as it is very insecure.

The ELXM-SW6 is designed for industrial client applications and can be either DIN-rail or panel mounted, and shock and vibration tested to IEC 60068.

The ELXM-SW6 is easy to use. Access the built-in webpages with any web browser to configure the ELXM-SW6 or use the Windows-based utility called *IH Browser*. It finds all the ProSoft Technology radios on the network and lists information about them. A topology view in the IH Browser shows how the wireless network is linked together at any point in time. Firmware and Configuration updates can be done at anytime from anywhere on the network. This includes over the wireless link or over the Internet.

EtherNet/IP™- or Modbus®-based PLCs/PACs can use message instructions to read diagnostic information from the radios, helping to reduce downtime when troubleshooting wireless network problems.

ProSoft Technology radios can easily be installed into new or existing systems.

Download sample programs, utilities, firmware images, and documentation from the ProSoft Technology website (www.prosoft-technology.com).

1.2.2 General Features

The ProLinx Edge™ Mini 802.11ax bridges are high-speed wireless Ethernet radios suitable for AGV roaming applications. Designed for industrial installations, the ELXM-SW6 offers many features including hazardous location certifications, Bridging, IGMP Snooping, OFDM for noise immunity, QoS, VLANs, RADIUS Server support, automatic parent selection for self-healing, OPC server diagnostics, extended temperature, high vibration/shock and DIN-rail mounting.

For individual radio product specifications and agency approvals, see Chapter *10 Appendix F - Detailed Radio Specifications*.

For LED descriptions, see section *4.2 LED Display*.

1.2.3 Antenna Port Connections

The ELXM-SW6 supports up to two antennas, configurable on the *Advanced Settings* page. Match the #antennas control (Port A or Port A – Port C) to the number of antennas in use. Antennas must be connected to the ELXM-SW6 when in use on the network.

Note: Antenna port B is currently not available on the ELXM-SW6. It is reserved for potential future use.

Mount antennas connected to the ELXM-SW6 so that polarization is the same. For remote placement of antennas, use an extension cable with an SMA-RP connector on the end connecting to the ELXM-SW6. Since the antenna cable attenuates the RF signal, use an antenna cable length that is only as long as necessary to ensure optimum performance.

Important: If the ELXM-SW6 is to be used in a hazardous location, the ELXM-SW6 must be mounted in an enclosure approved for hazardous locations.

The ELXM-SW6 has active antenna connectors on the front as shown below:

Radio	Antenna Connectors A & C
ELXM-SW6 • 2 Active Antenna Ports • Allows MIMO operation	

1.3 Package Contents

1.3.1 ELXM-SW6

The following components are included with standard ELXM-SW6 products:

Qty.	Part Name	Part Number	Part Description
1	ELXM-SW6	*Varies*	ProLinx Edge™ Mini 802.11a, b, g, n, ac, ax
1	Power Connector	350-1021	Mating power connector for the ELXM-SW6, for attachment to customer's power supply.

Download sample programs, utilities, firmware images, and documentation from the ProSoft Technology website (www.prosoft-technology.com).

1.4 Installing the Industrial Hotspot Browser

Use the *Industrial Hotspot Browser* Configuration Tool (hereafter called the *IH Browser*) to set up and configure the ELXM-SW6. It is designed for personal computers running the Microsoft Windows operating systems.

1.4.1 IH Browser System Requirements

The IH Browser is designed to run on Microsoft Windows™ and supports Windows™ 10 and 11.

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

1.4.2 Installing IH Browser Software

The *Industrial Hotspot Browser* (IH Browser) software must be installed to configure the ELXM-SW6 as it is not shipped with a default static IP Address.

To install IH Browser from the ProSoft Technology website

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

2 ELXM-SW6 Quick Setup

This chapter describes how to set up ELXM-SW6's in a minimal configuration before deploying them in the permanent installation. The procedures in this section cover basic configuration and how to verify successful operation.

The procedures described in this section assume the ELXM-SW6 is in its default configuration as shipped by ProSoft Technology. If that is not the case, reset the ELXM-SW6 to factory defaults before attempting these procedures. For more information, please see section *4.3.1 Resetting to Factory Defaults*.

Note that in any given network, there must be at least one radio acting as an 802.11 Access Point, either from ProSoft Technology or a 3rd party vendor. ELXM-SW6's configured as Clients will connect wirelessly to the Access Point to form a network bridge between their Ethernet interfaces.

If possible, having a test Access Point configured the same as Access Points in the permanent installation as part of the Configuration Environment will confirm that the Client radios are configured correctly.

If replacing an existing radio with a new radio of the same type, see section *2.7 Replacing an Existing ELXM-SW6*.

2.1 Preparing the Configuration Environment

If an Access Point is not nearby to test the wireless connection or the Access Point is very close by (5 to 10 feet), antennas may not be needed on the ELXM-SW6 for this procedure as it may have sufficient signal strength to link over short distances.

Tip: To make it easier to physically identify the ELXM-SW6, apply a label to each ELXM-SW6 indicating the radio name and IP address.

2.2 Making Power and Data Connections

2.2.1 ELXM-SW6 Connections

The power and Ethernet connections are located on the front of the case.

1. If testing the wireless connection with an Access Point, ensure it is nearby, powered up and operational.
2. Attach an Ethernet cable from the PC or laptop to the ELXM-SW6. Either assign a static IP Address to the PC's Ethernet port or allow a minute or two for the Windows Automatic Private IP Addressing to assign the Ethernet port an IP Address in the 169.254.xx.xx subnet.
3. Connect a power cable (power connector included with the ELXM-SW6) to the Power port.
   - The RJ45 connector Ethernet ACTIVITY LED illuminates when data is sent to or received from the ELXM-SW6 Ethernet interface.
   - The RJ45 connector Ethernet LINK LED indicates the speed of the Ethernet connection:

SPEED LED	Ethernet Connection speed
LED is off	10 Base T
LED is on	100 Base T
LED blinks about once every two seconds	1000 Base T

2.3 ELXM-SW6 Power-Up

The ELXM-SW6 boots-up when power is supplied to the ELXM-SW6 - there is no On/Off switch.

a) The POWER LED lights amber when power is applied.

b) The POWER LED switches to green and the bottom SIGNAL STRENGTH LED lights amber briefly.

c) The bottom SIGNAL STRENGTH LED turns off.

d) ACTIVITY LED starts flashing green.

This process takes 10 to 15 seconds. Once the ACTIVITY LED is flashing green, the ELXM-SW6 is operational. Other LEDs on the ELXM-SW6 may become active as well.

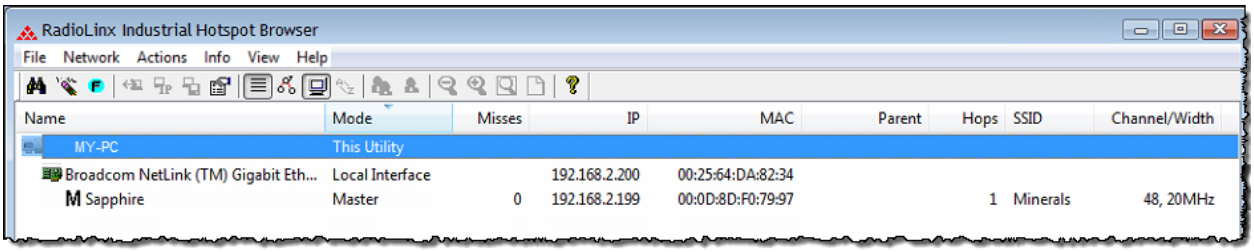
Please note the MAC address of the ELXM-SW6 is printed on a label attached to the front. The MAC address has the form 00-0D-8D-F4-YY-ZZ. For example, 00-0D-8D-F4-5C-8E. Use this number to identify the ELXM-SW6 on the network when using the IH Browser.

2.4 Using the IH Browser to Configure Radios

This section describes how to use IH Browser to set up an ELXM-SW6 in a minimal configuration before deploy in a permanent installation.

2.4.1 Viewing the ELXM-SW6 in the IH Browser

Start the IH Brower. If the ELXM-SW6 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 ELXM-SW6. The *List* view (shown in the image below) displays the ELXM-SW6 (or previous generation RLX2 radio) on the same network as the computer running the IH Browser. In this case, with a direct Ethernet cable connection between the PC and the ELXM-SW6 there should only be one device shown.



Note: Perform many common tasks by right-clicking on the ELXM-SW6 and choosing a command.

2.4.2 Refreshing the Display in the IH Browser

If changes are made to the ELXM-SW6's configuration, 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 ELXM-SW6's (or from the **FILE** menu choose **SCAN**).

2.4.3 Setting the ELXM-SW6 IP Address in the IH Browser

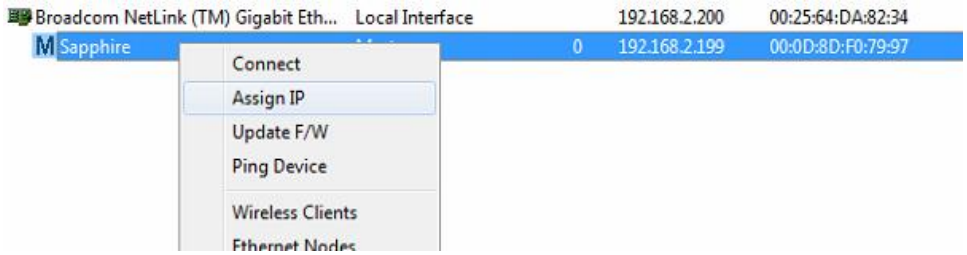
If the ELXM-SW6 is on and connected to a network with a DHCP server, it gets an IP address through DHCP.

If the ELXM-SW6 is not on a network with a DHCP server, the ELXM-SW6 appears with an IP address of **0.0.0.0**. Assign a temporary IP address to assist with configuring the ELXM-SW6.

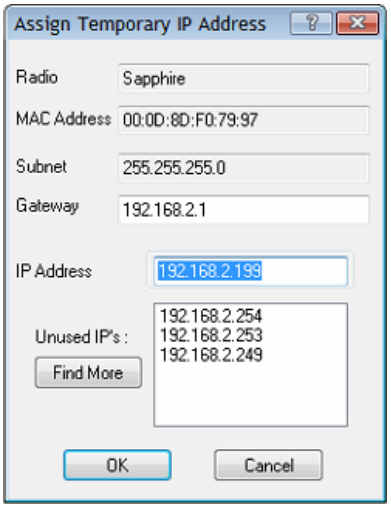
2.4.4 Assigning a Temporary IP Address

A temporary IP address provides access to configure the ELXM-SW6 when it 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 ELXM-SW6 and then click **ASSIGN IP**.

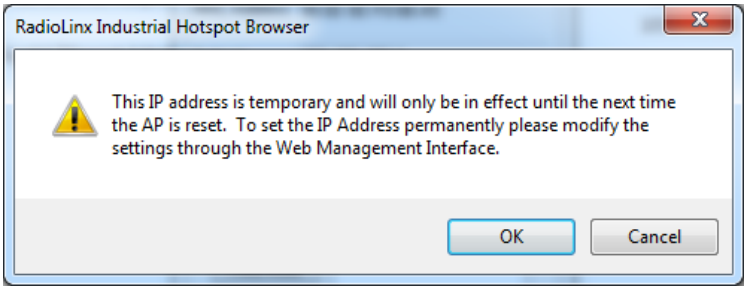


This opens the *Assign Temporary IP Address* dialog box.



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

2 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 IP addresses, or enter an unused IP address, and then click **OK**. The IH Browser warns that the IP address is temporary.



3 Click **OK** and then refresh the display in the IH Browser. The ELXM-SW6 should now appear in the IH Browser window with the temporary IP address.

4 To set a static IP address for the ELXM-SW6, see section *3.5.2 Access Settings*.

2.5 Configuring an ELXM-SW6 - Getting Started

This section describes how to set up an ELXM-SW6 in a minimal configuration before deploying them in the permanent installation. See Chapter *3 Configuring the ELXM-SW6 - Detailed Configuration* for a detailed description of all the configuration parameters available for the ELXM-SW6.

2.5.1 Connecting to the ELXM-SW6 Configuration Interface

This section describes how to connect to the ELXM-SW6 Configuration / Diagnostic web interface using a web browser such as Internet Explorer or Firefox.

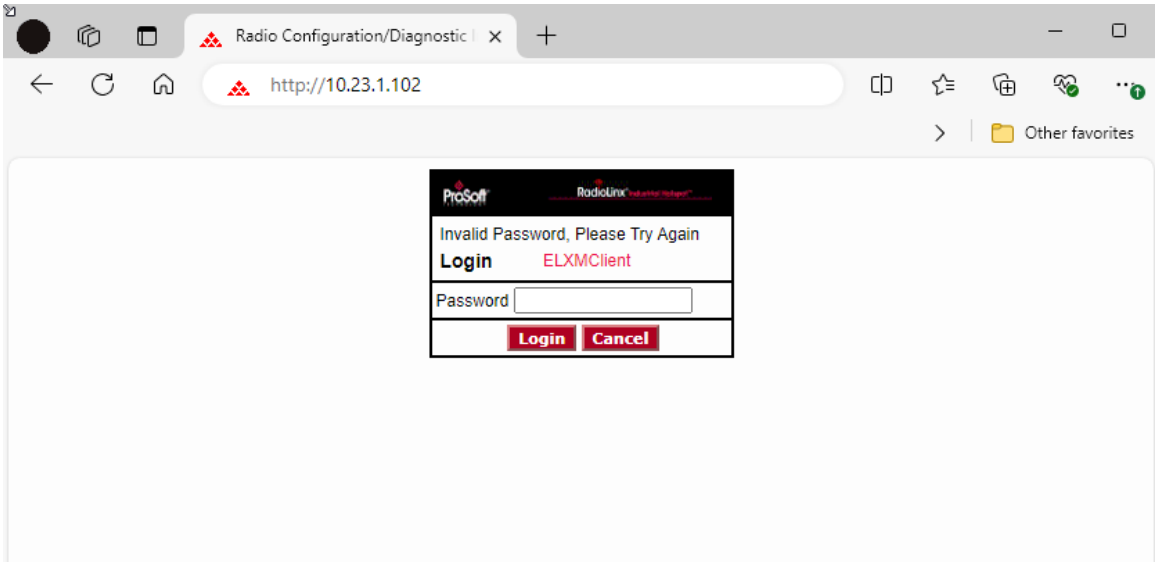
Important: The computer or other device must be connected to the same network as the ELXM-SW6.

1 Log into the web interface of the ELXM-SW6. Do this in any of three ways:

- In the IH Browser List view or Topography view, right-click the ELXM-SW6 and then click **CONNECT**.
- In the IH Browser List view or Topography view, double-click the ELXM-SW6.
- Open a web browser on your PC and enter the IP address for the ELXM-SW6. For example: `http://192.168.6.10`

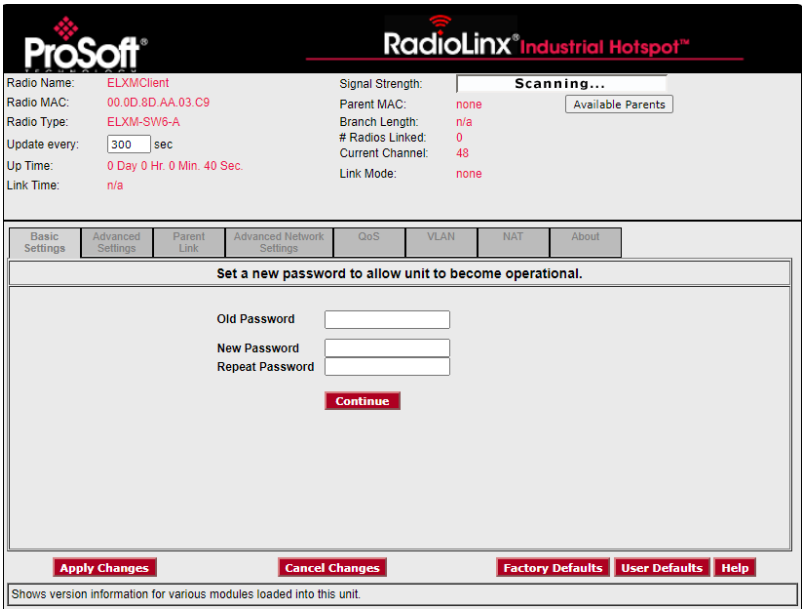
Then press **ENTER**.

2 The login screen appears in the web browser.



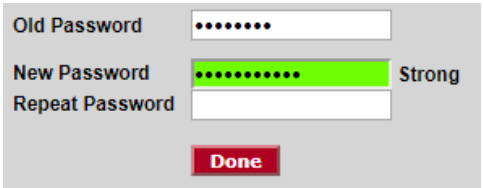
4 Enter the password and then click **LOGIN**. The default password is *password*. If the password is lost, the ELXM-SW6 can be reset to its default settings. For more information, see section *4.3.1 Resetting to Factory Defaults*.

5 If the ELXM-SW6 is set to its factory settings or has been reset to defaults, a new password is required before the configuration tabs are enabled. This is to ensure that the ELXM-SW6 is not unintentionally put into operation using the factory default password.

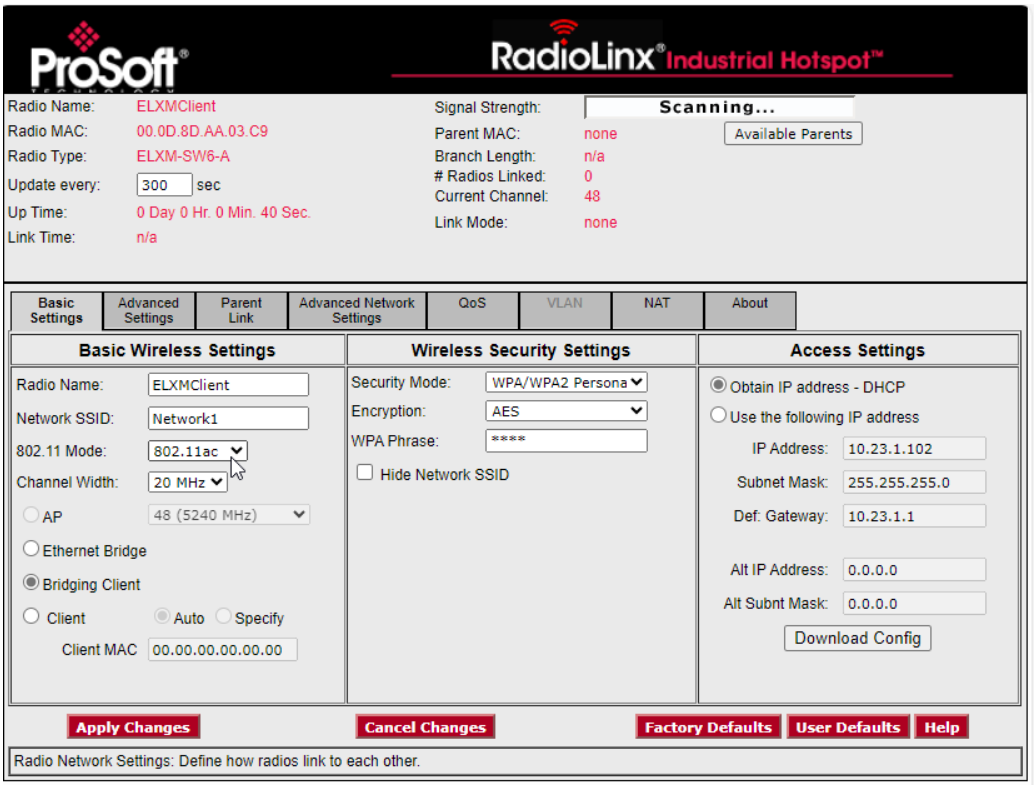


Enter the default password into the **OLD PASSWORD** edit box, then a password with sufficient security strength into the **NEW PASSWORD** edit box. The new password must be satisfy the following:

- Must contain both lower and upper case letters
- Must contain one or more numbers
- Must contain at least one non-alphanumeric character (e.g. !@#$).
- Must be at least 8 characters in length



6 Click the **CONTINUE** button to open the main configuration webpage of the ELXM-SW6.



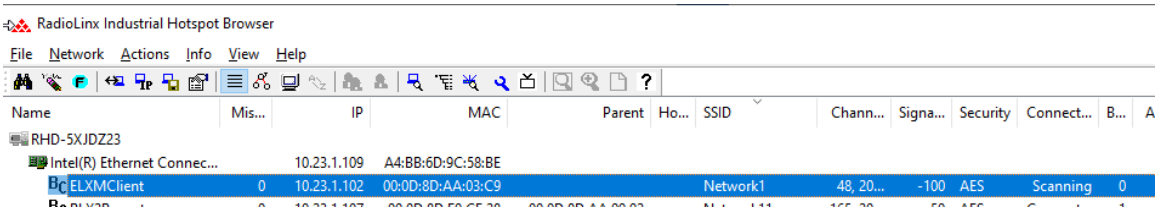
Note: Some parameters may be different from the image above, depending on the specific ELXM-SW6 model.

Tip: The help topic can be displayed for any parameter in the ELXM-SW6 webpage by clicking the parameter name. There is also a short description at the bottom of the window.

2.5.2 Configuring as a Bridging Radio

If the wireless network is using ProSoft Technology RLX2 radios as the Access Points, the ELXM-SW6 must be configured into its Ethernet Bridging mode.

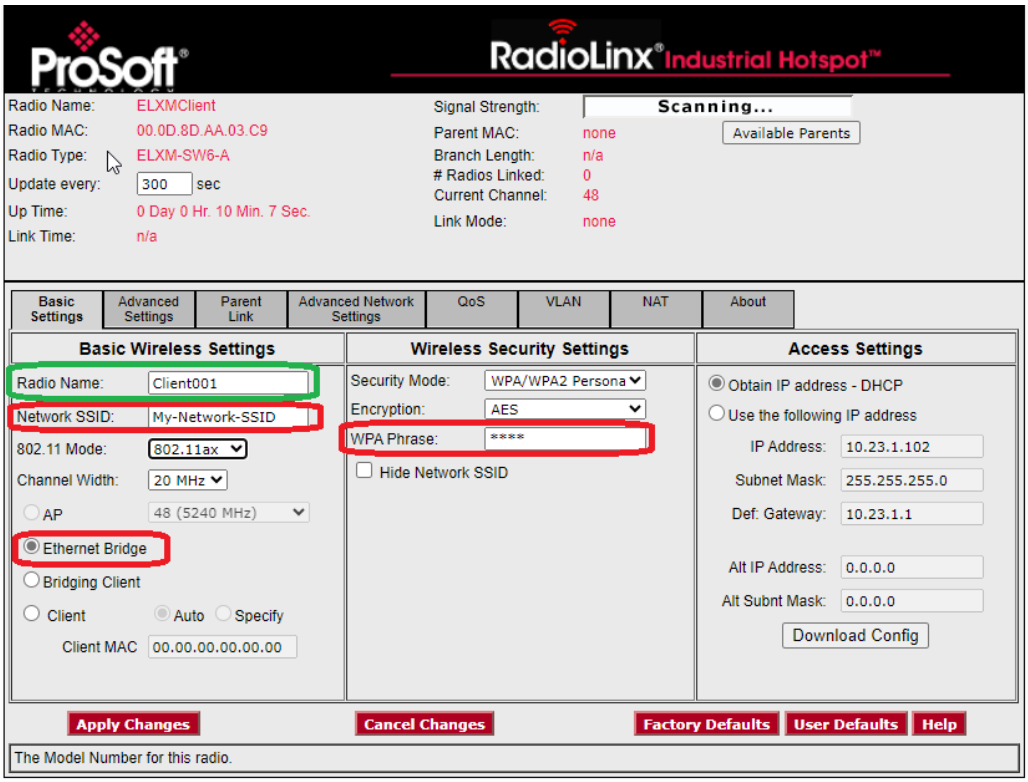
1 Start the IH Browser on the PC connected to the ELXM-SW6 Ethernet port. After the ELXM-SW6 starts, it should appear in the IH Browser.



2 If the ELXM-SW6 IP address is **0.0.0.0**, assign a temporary IP address to the ELXM-SW6. For more information, see section *2.4.4 Assigning a Temporary IP Address*. In this example, the ELXM-SW6 has an IP address of **10.23.1.102**.

3 Log into the ELXM-SW6's web interface. For more information, see section *2.5.1 Connecting to the ELXM-SW6 Configuration Interface*.

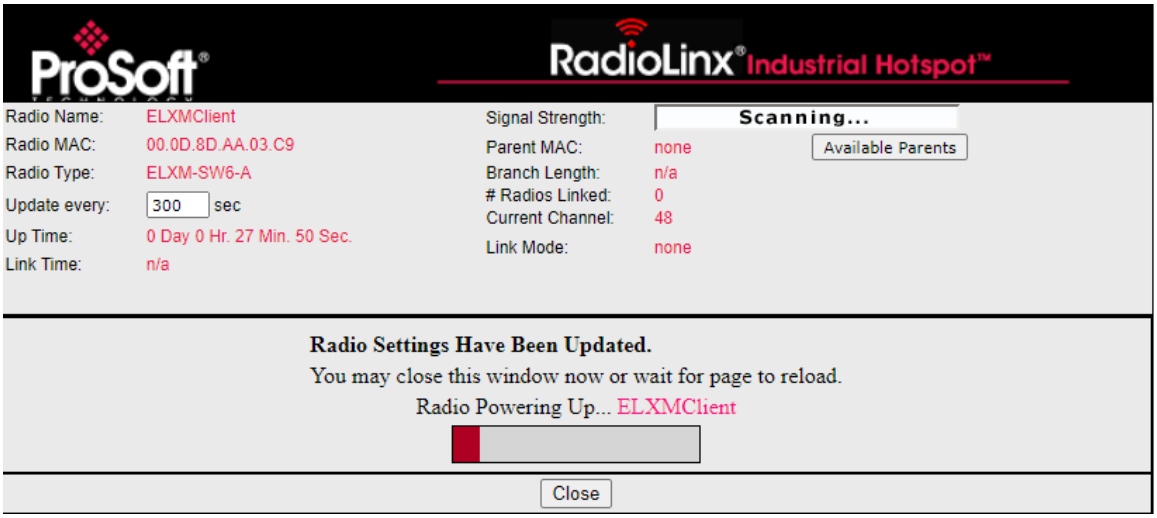
The fields highlighted in red must be set as a minimum for the ELXM-SW6 to connect to a ProSoft Technology Access Point.



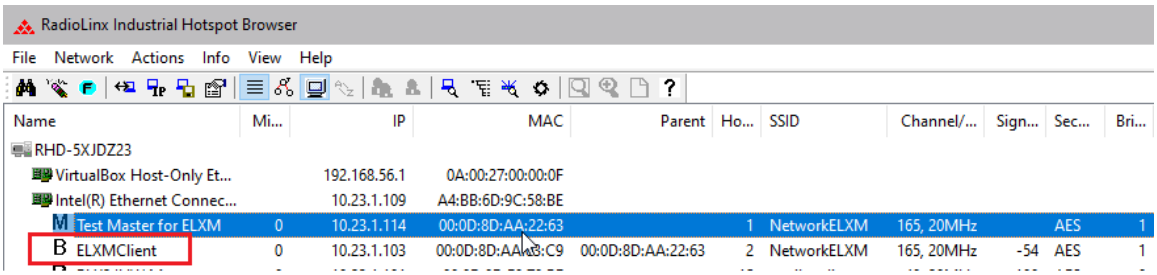
4 On the **BASIC SETTINGS** tab, in the **BASIC WIRELESS SETTINGS** group, change the ELXM-SW6 to **ETHERNET BRIDGE** and set the **WPA PHRASE** and **SSID** to match that of the Access Points with the same SSID.

5 Although not strictly necessary, set the **RADIO NAME** to something unique (e.g. Client001 as shown above).

6 Click **APPLY CHANGES** to reboot the ELXM-SW6.



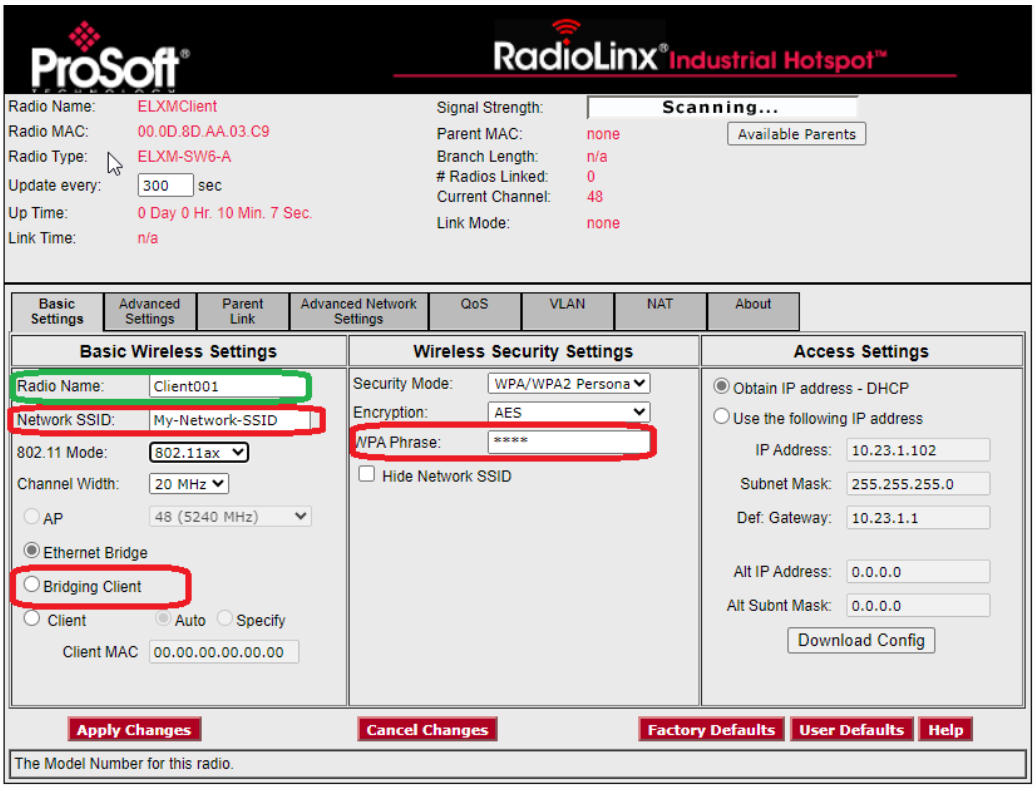
7 After successfully rebooting, the ELXM-SW6 appears as an Ethernet Bridge radio in the IH Browser window:



2.5.3 Configuring as a Bridging Client Radio

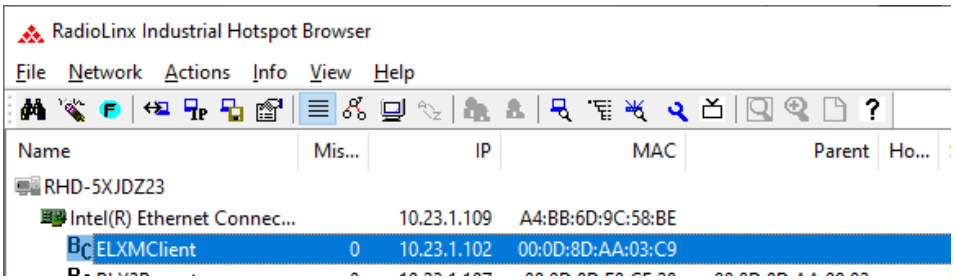
The ELXM-SW6 can be configured in Client or Bridging Client modes for third-party 802.11 Access Point connections. See section *2.5.4 Configuring as a Client Radio* for the differences in the modes. The following example assumes that there is a PC connected via Ethernet cable to the ELXM-SW6's Ethernet port.

1. Power up a new ELXM-SW6 in the default configuration.
2. Start the IH Browser. After the ELXM-SW6 starts, it should appear in the IH Browser.
3. In the IH Browser, assign a temporary IP address to the ELXM-SW6. For more information, see section *2.4.4 Assigning a Temporary IP Address*.
4. Log into the ELXM-SW6. For more information, see section *3.1 Connecting to the ELXM-SW6 Configuration Interface*.
5. On the **BASIC SETTINGS** tab, in the **BASIC WIRELESS SETTINGS** group, change the ELXM-SW6 to **BRIDGING CLIENT** and set the **RADIO NAME, WPA PHRASE** and **SSID** accordingly.



6. Click **APPLY CHANGES** to save the configuration.

7 Refresh the display in the IH Browser. The ELXM-SW6 appears in the IH Browser as a Bridging Client radio:



8 If there is an AP with the correct credentials nearby, the Bridging Client should wirelessly connect. In this mode, multiple Ethernet devices can connect with any 3rd-party access points (802.11 a/b/g/n/ac/ax).

2.5.4 Configuring as a Client Radio

The ELXM-SW6 can be configured in *Client* mode for third-party 802.11 Access Point connections and supports applications using non-IP based protocols. The following table highlights the most significant differences between Bridging, Client, and Bridging Client modes on the ELXM-SW6.

	Bridging	**Client**	**Bridging Client**
Number of attached Ethernet devices supported	Multiple (up to the limits of network)	One	Multiple (up to 16)
Can other wireless devices connect to the ELXM-SW6?	No	No	No
Can the ELXM-SW6 connect to non-ProSoft Technology Access Points	No	Yes	Yes
MAC Addresses seen by Access Point	All MAC Addresses	Only the MAC address of the connected Ethernet device or the user-specified MAC address.	Only the ELXM-SW6's MAC address

Client mode is a special mode in the ELXM-SW6 that allows a user to connect an Ethernet device to a wireless network through any 802.11a, b, g, n, ac or ax access point. Any Ethernet device that has an RJ45 Ethernet port can, in effect, become an 802.11 wireless client by attaching the ELXM-SW6. Only a single device can be connected to the ELXM-SW6 in Client mode. Do not connect to more than one Ethernet device (using a switch or hub).

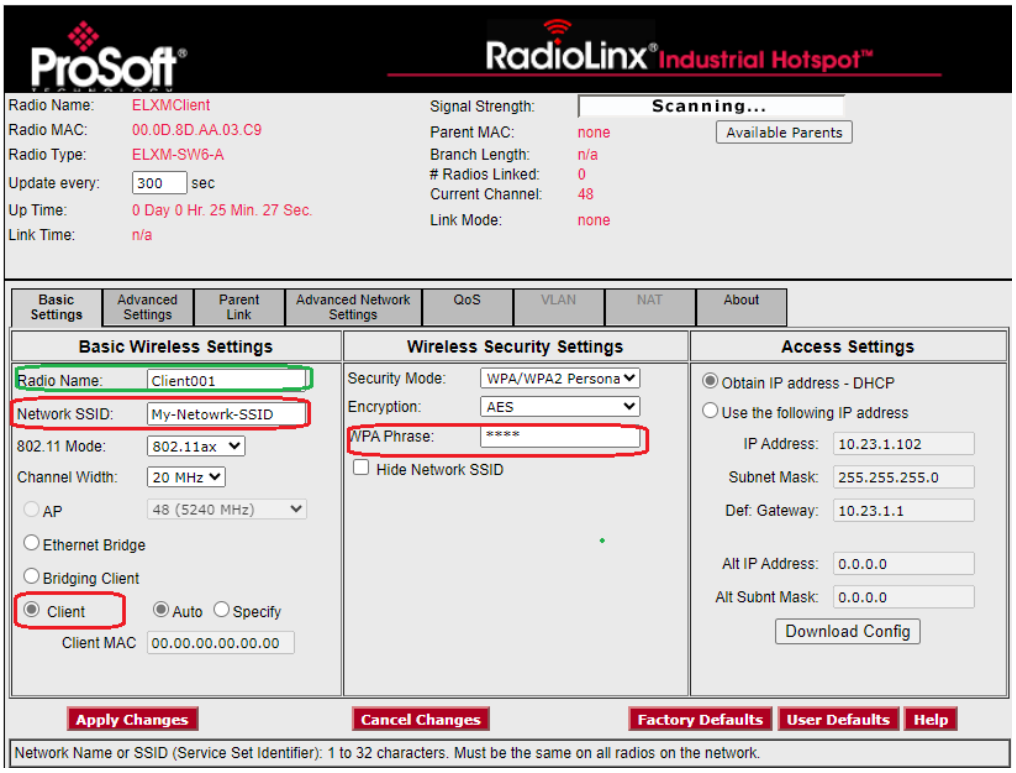
Note: Only use client mode to connect to another brand access point **and** the application is using non-IP based protocols.

If ProSoft Technology Radios are used as Access Points, always use the ELXM-SW6 in Bridging mode which transparently transports all Ethernet frames at the MAC level (layer 2 bridging). If a Client ELXM-SW6 is not needed in the system, skip the following example configuration.

The following example assumes there is a PC connected via Ethernet cable to the ELXM-SW6's Ethernet port.

1. Power up a new ELXM-SW6.
2. Start the IH Browser. After the ELXM-SW6 starts, it should appear in the IH Browser.
3. In the IH Browser, assign a temporary IP address to the ELXM-SW6. For more information, see section *2.4.4 Assigning a Temporary IP Address*.
4. Log into the ELXM-SW6. For more information, see section *3.1 Connecting to the ELXM-SW6 Configuration Interface*.

5 In the **BASIC WIRELESS SETTINGS** group, change the ELXM-SW6 to **CLIENT**.

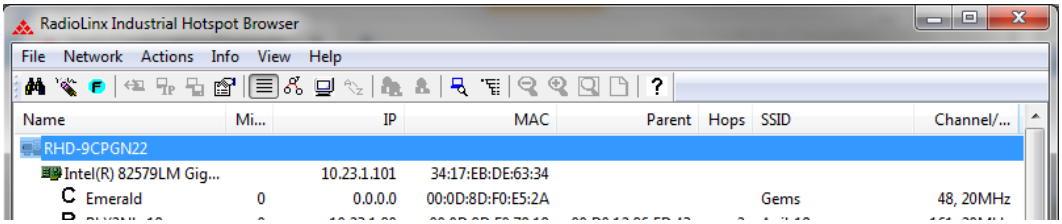


6 Set the **RADIO NAME, WPA PHRASE** and **SSID** accordingly.

7 Set the permanent IP address. On the **BASIC SETTINGS** tab, in the **ACCESS SETTINGS** group, click **OBTAIN IP ADDRESS - DHCP** or **USE THE FOLLOWING IP ADDRESS**.

8 Click **APPLY CHANGES** to reboot the ELXM-SW6. A progress bar displays during reboot.

9 Refresh the display in the IH Browser. The ELXM-SW6 appears in the IH Browser as a Client radio.



10 When the Client radio reboots, wait until the ELXM-SW6 registers the MAC address of the PC's Ethernet interface (Client mode only).

11 Ensure that the PC's IP address is on the same subnet as the AP network for the SSID.

2.6 Viewing the ELXM-SW6 Configuration

To quickly view an ELXM-SW6 configuration:

1. Start the IH Browser.
2. Right-click the ELXM-SW6 and then click **PROPERTIES**.
3. To view all the available properties, in the *Detailed Information for Radio* dialog box, click **MORE**. The ELXM-SW6's configuration cannot be changed in this dialog box.
4. To change the configuration, or view more details, see section *2.5 Configuring an ELXM-SW6 - Getting Started* or Chapter *3 Configuring the ELXM-SW6 - Detailed Configuration*.

2.7 Replacing an Existing ELXM-SW6

The ELXM-SW6 supports easy replacement either by uploading a previously saved configuration file using the IH Browser, or via a microSD card in the back of the ELXM-SW6.

The ELXM-SW6 supports moving the configuration from an installed ELXM-SW6 to a replacement using a microSD card. This feature reduces the time to replace a damaged ELXM-SW6.

Remove the microSD card from the existing ELXM-SW6 and install it in the new ELXM-SW6. When the new ELXM-SW6 is powered up, it reads the configuration stored on the microSD card, detects that it differs from the operating configuration and adopts it.

By default, the ELXM-SW6 writes configuration changes to an inserted microSD card (Personality Module) when configuration changes are made.

Important: While this feature can save time replacing an ELXM-SW6 in the field, it is also a potential security risk. The configuration stored on the microSD could be inserted into another ELXM-SW6, and the ELXM-SW6 could then access the network.

The file on the microSD card is encrypted so the configuration information (principally the configuration password and encryption key) cannot be extracted. It is highly recommend to physically secure the ELXM-SW6 and the microSD card.

If the Personality Module feature is not used, it is recommended to turn off the SD Auto-Clone Enable and SD Auto-Write Enable parameters. For more information, please see section *3.6.4 Personality Module Settings*.

Important: Before installing a new ELXM-SW6, please verify that all listed product items are present. For more information, please see section *1.3 Package Contents*.

3 Configuring the ELXM-SW6 - Detailed Configuration

The ELXM-SW6 includes a built-in Web Server that to configure and monitor the ELXM-SW6. The webpages can be displayed from any computer that can connect to the ELXM-SW6 through a wired Ethernet connection or a wireless connection.

3.1 Connecting to the ELXM-SW6 Configuration Interface

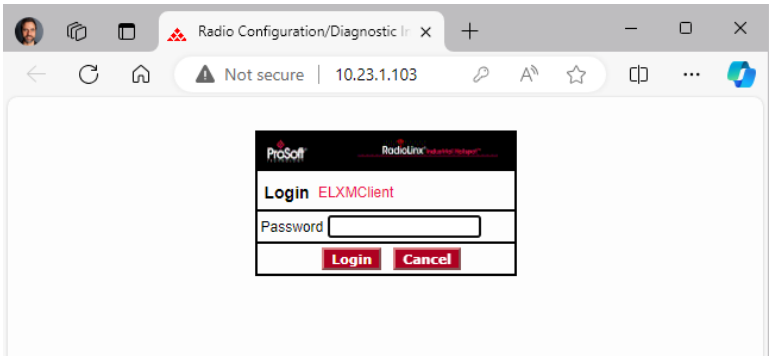
This section describes how to connect to the ELXM-SW6 using a web browser from a PC or other network-enabled device.

Important: The PC or other device must be connected to the same network as the ELXM-SW6.

1 Log in to the ELXM-SW6 in any of three ways:

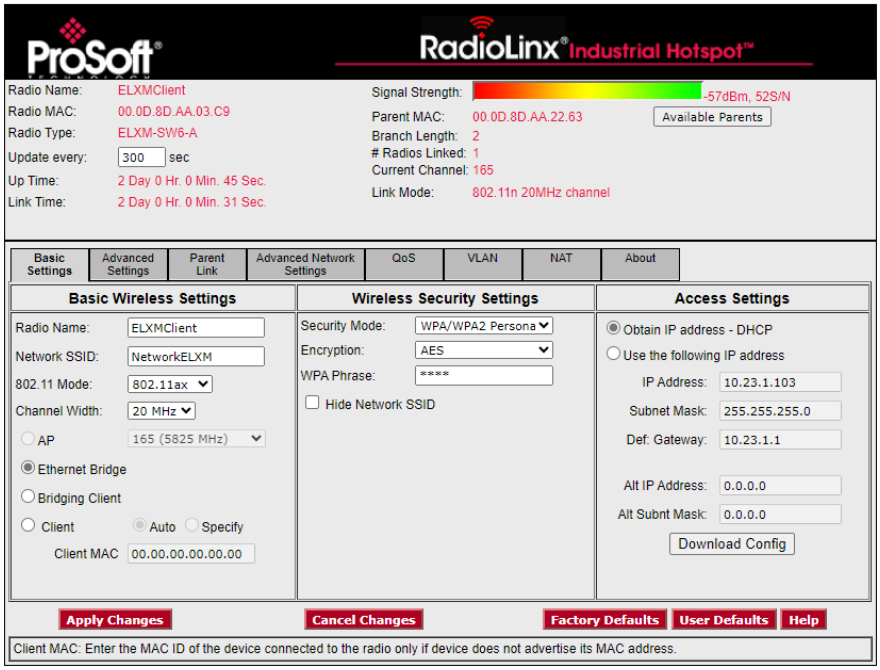
- In the IH Browser *List* view or *Topography* view, right-click the ELXM-SW6 and then click **CONNECT**.
- In the IH Browser *List* view or *Topography* view, double-click the ELXM-SW6.
- Open a web browser on the PC, enter the ELXM-SW6's IP address, and then press **ENTER**. For example, `http://192.168.6.10`.

The login screen appears in the web browser.



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

If the ELXM-SW6 password is lost, the ELXM-SW6 can reset to its default settings. For more information, please see section *4.3 Resetting the ELXM-SW6 to Defaults*. This opens the main configuration webpage for the ELXM-SW6. Note that some parameters may be different from the image depending on the specific ELXM-SW6 model.



Tip: Display the help topic for any parameter on the webpage 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 at the bottom of the window.

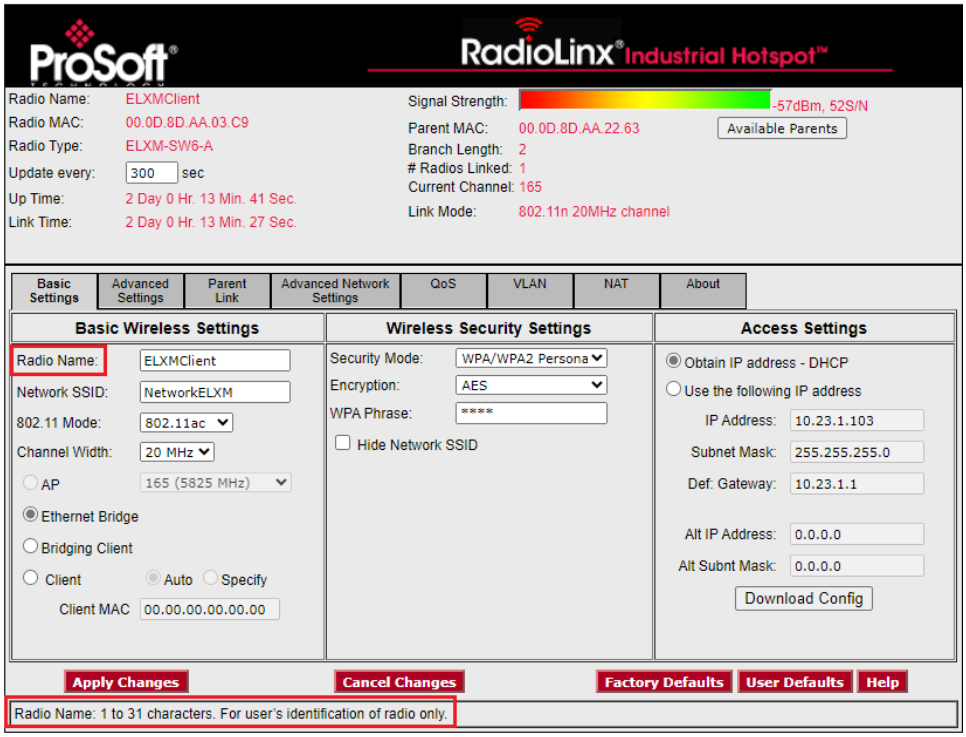
3.1.1 Read-Only Fields

Some of the parameters are for display, and only provide information about the current state of the ELXM-SW6.

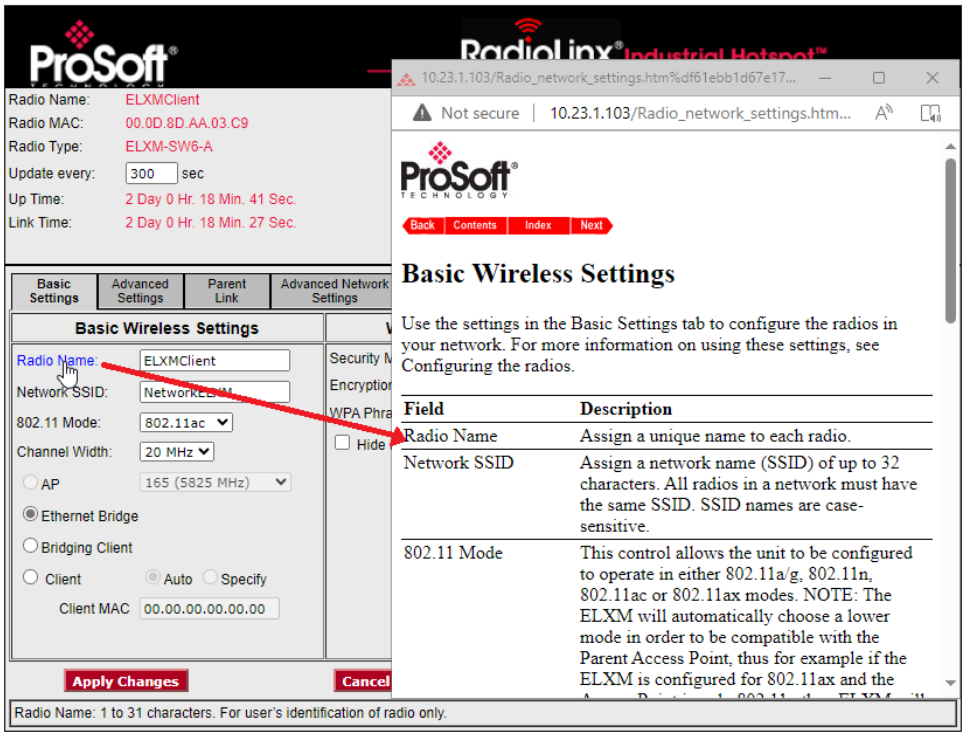
Depending on the model of the ELXM-SW6 and its configuration, some parameters and buttons may not be available or appear on the page.

3.1.2 Configuration Help

Help is available for each item on the page. To view a brief help message about any parameter on the screen, move the cursor over the parameter until the parameter name turns blue, or press the **TAB** key to select the parameter. Refer to the text at the bottom of the screen.



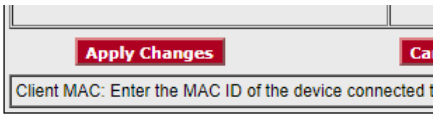
To view more information about the selected parameter, click the parameter name. This opens a help page in a new browser window.



To view the complete online documentation for the ELXM-SW6, click the Help button. This opens the online documentation in a new browser window.

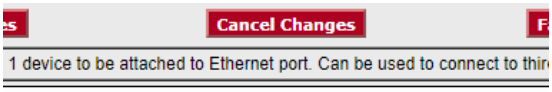
3.1.3 Apply Changes

Click **APPLY CHANGES** to save changes to the ELXM-SW6 configuration and restart the ELXM-SW6 with the new configuration.



3.1.4 Cancel Changes

Click **CANCEL CHANGES** to discard any configuration changes made during this session.



Note: This button only applies to changes made since the **APPLY CHANGES** button was last clicked.

A similar action can be achieved by Refreshing the page on the web browser.

3.1.5 Factory Defaults

Click **FACTORY DEFAULTS** to reset the ELXM-SW6 to the original factory default settings.

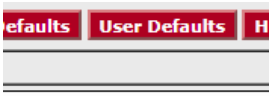
Important: This action discards all changes made to the ELXM-SW6 configuration settings.

If there is a microSD card in the ELXM-SW6's Personality Module slot:

- Clicking **FACTORY DEFAULTS** does not reset the configurations stored on the microSD card in the ELXM-SW6's Personality Module slot.
- If **SD AUTOWRITE ENABLE** is selected on the **ADVANCED SETTINGS** tab, the ELXM-SW6 overwrites the configuration on the microSD card with the factory default settings when **APPLY CHANGES** is clicked. For more information, please see section *3.6.4 Personality Module Settings*.

3.1.6 User Defaults

Click **USER DEFAULTS** to reset the ELXM-SW6 to the last user defaults configuration file that was uploaded into the ELXM-SW6.



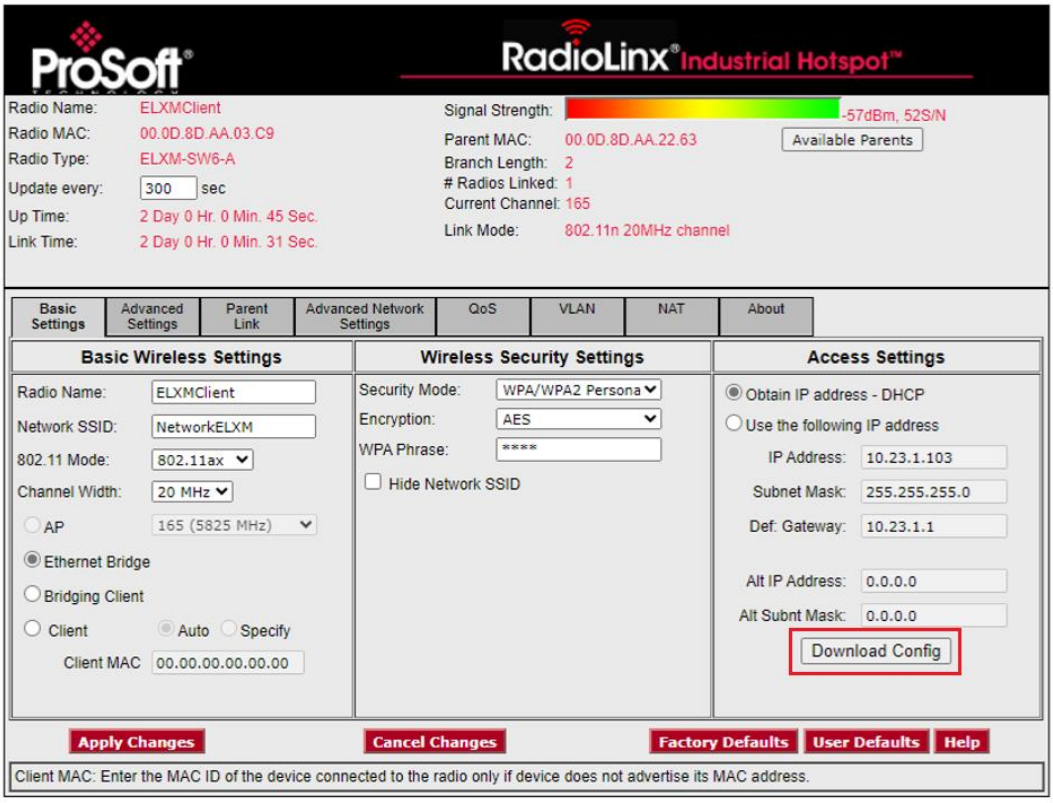
Important: If a User Default configuration has not been loaded into the ELXM-SW6, then clicking the **USER DEFAULTS** button will have the same effect as clicking the **FACTORY DEFAULTS** button.

See section *3.1.6.1 Uploading User Defaults to an ELXM-SW6* for instructions on creating a user default configuration file and how to save it in the ELXM-SW6.

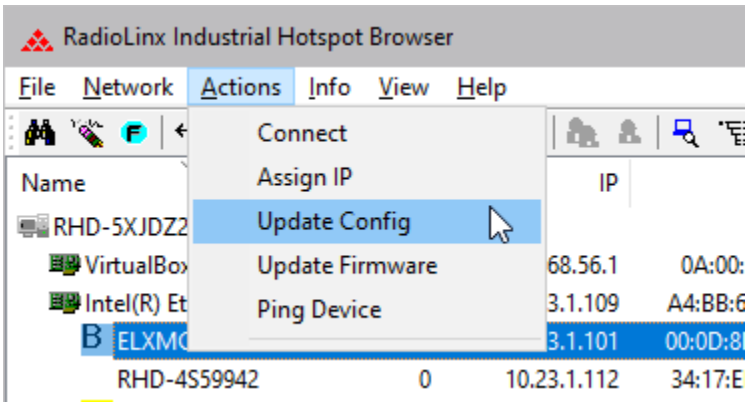
3.1.6.1 Uploading User Defaults to an ELXM-SW6

This section covers the creation of a user default configuration file and how to save it in the ELXM-SW6.

1. Manually configure an ELXM-SW6 with the desired settings for the application.
2. Download the configuration file from the ELXM-SW6 by clicking the **DOWNLOAD CONFIG** button in the *Basic Settings* > *Access Settings* tab.

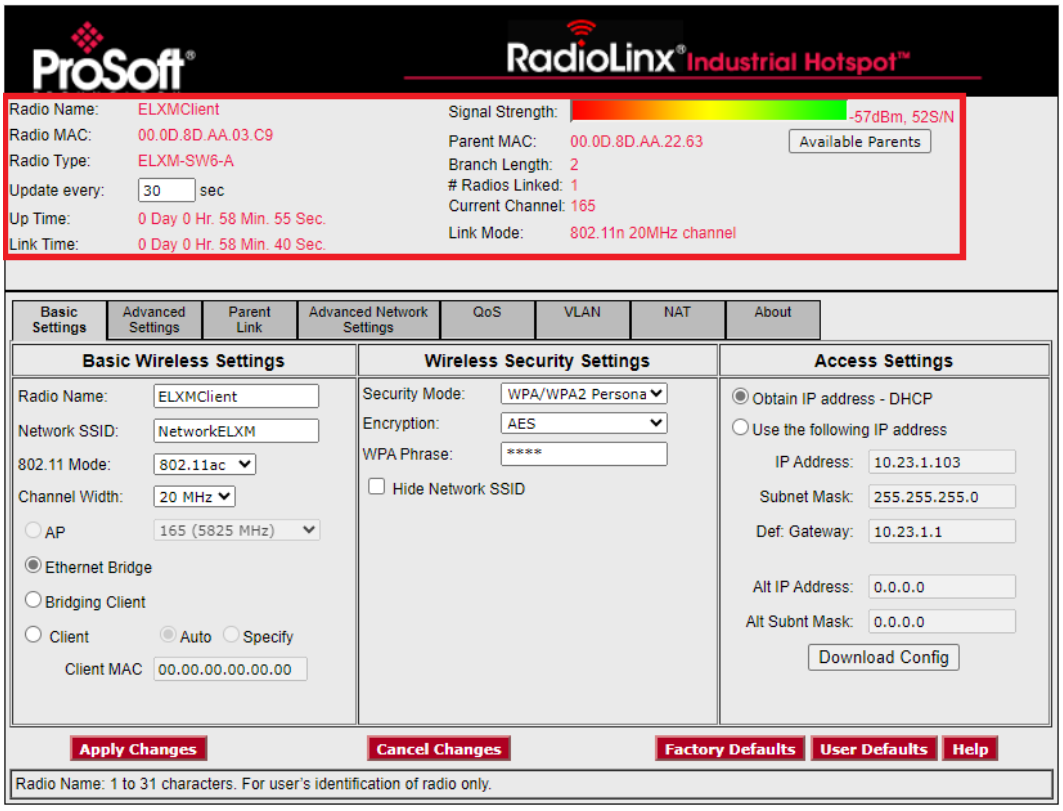


3 In the IH Browser, click on **ACTIONS** > **UPDATE CONFIG** option to upload the configuration file to one or more of the ELXM-SW6 radios.



3.2 Viewing ELXM-SW6 Status

The ELXM-SW6 status parameters appear at the top of the ELXM-SW6 webpage.



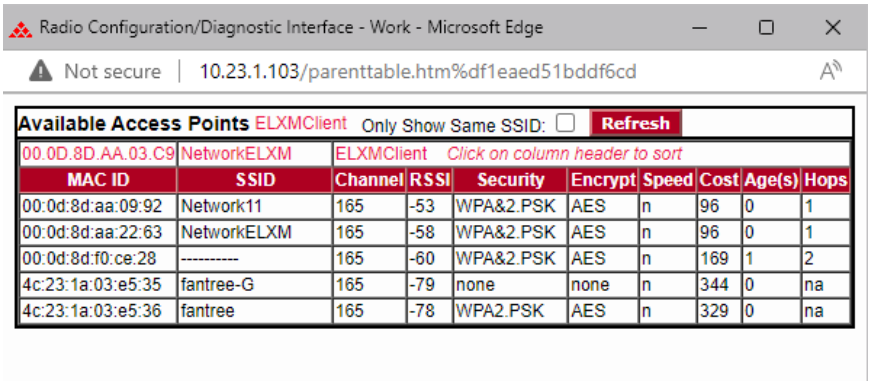
Note: Different versions of the ELXM-SW6 and firmware support different functions. There may be fewer or more parameters on this page, depending on the version of the ELXM-SW6 and firmware.

Most of the parameters in the ELXM-SW6 status area are read-only and display the current settings and status for the ELXM-SW6.

Parameter	Description
Radio Name	The user-assigned name for the ELXM-SW6.
Radio MAC	MAC address of the selected ELXM-SW6. The MAC ID is also printed on the side of the ELXM-SW6.
Radio Type	The Model Number of the ELXM-SW6. For example: *ELXM-SW6-A*, or *ELXM-SW6-E*
Update every	The number of seconds the webpage waits between refreshing the data. To change the value temporarily, enter the new value and press the **TAB** key.
Up Time	The length of time the ELXM-SW6 has operated since the last system power-up or reset.
Link Time	The length of time that the ELXM-SW6 has been continuously connected to the parent.
Signal Strength	The strength of the signal from the parent in dBm units as well as the relative S/N (Signal to Noise).
Parent MAC	The MAC address of the parent to which the ELXM-SW6 is linked.
Branch Length	The number of RF links from the ELXM-SW6 to the Master radio.
# Radios Linked	The number of other radios that are linked to the ELXM-SW6.
Current Channel	The current operating channel for the ELXM-SW6. For an AP radio, this is the channel set in the *Basic Wireless Settings*. For a Client radio, this is the same channel as the linked parent. When the *Link Mode* parameter shows that the ELXM-SW6 is in 40 MHz mode, this parameter shows the main channel number, followed by the extension channel's number.
Link Mode	The 802.11 Mode in which the ELXM-SW6 is operating (a/b/g/n/ac/ax). For an AP radio, this is the highest mode supported. For a Client radio, this is the highest common mode supported by both: The settings of the Client radio and its parent The capability of the radio channel.
Available Parents	Click this button to view the list of Access Points and Bridges (Parents) from which the ELXM-SW6 can detect beacons. This button is only available when the ELXM-SW6 is in a Client mode (set in the *Basic Wireless Settings*). For more information, see section *3.2.1 Viewing Available Parents for a ELXM-SW6*.

3.2.1 Viewing Available Parents for a ELXM-SW6

To view the *Available Access Points* table, click **AVAILABLE PARENTS**. This table is only available when the ELXM-SW6 is in Bridge or a Client mode.



This page is helpful for viewing:

- The possible parents for the ELXM-SW6 when in Bridge or Client mode. The current parent should normally be the ELXM-SW6 with the lowest cost and a matching SSID.
- Other 802.11 networks in the area.

Note: Click on a column header to sort the table by the values in that column.

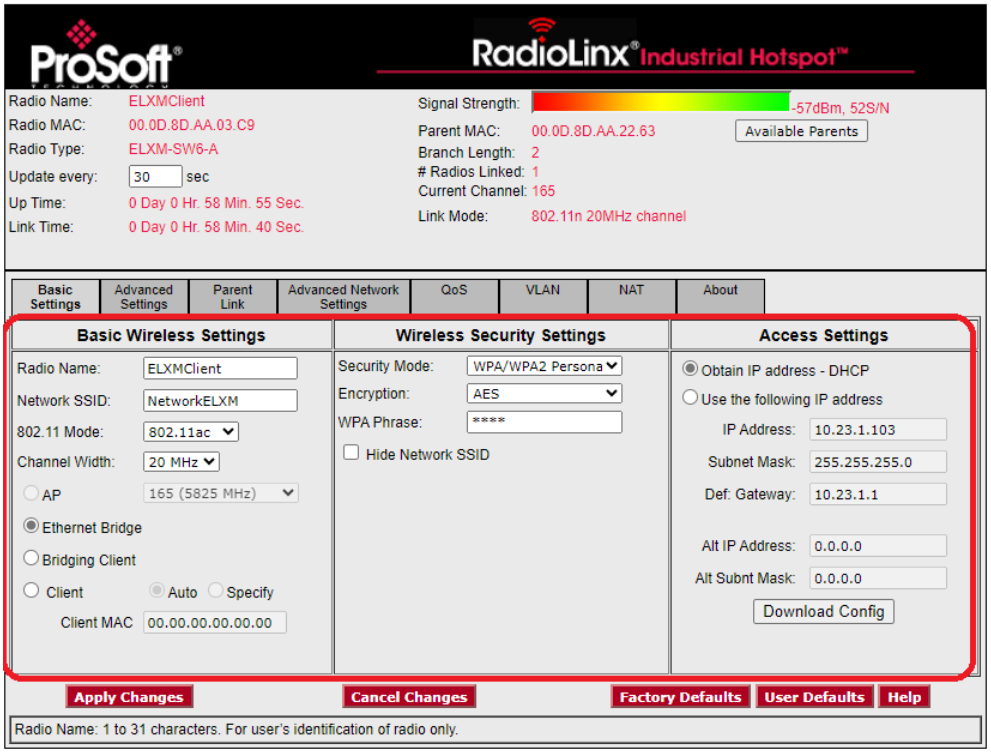
Parameter	Description
Only Show Same SSID	Select this check box to restrict the list of available parents to those with the same SSID as the ELXM-SW6 to be configured.
Refresh	Click this button to re-scan the network and update the devices in the list.
Mac ID	Displays the unique hexadecimal MAC Address of the detected device.
SSID	Displays the network name (Service Set Identifier) that the device is advertising.
Channel	The radio channel on which the device is transmitting. The band (2.4 GHz or 5 GHz) can be derived from the channel number. Channel < 15 => 2.4 GHz Channel > 15 => 5 GHz
RSSI	Displays the Received Signal Strength in dBm.
Security	Displays the security mode enabled for the device.
Encrypt	Displays the encryption type enabled for the device
Speed	Displays the IEEE 802.11 connection speed (a, b, g, n, ac or ax). The ELXM-SW6 supports all these 802.11 connection speeds.
Cost	Displays the calculated parent selection cost. The ELXM-SW6 evaluates the link it has to its parent once per second to determine if this link is the best parent to use. The ELXM-SW6 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.
Age(s)	Displays the length of time (in seconds) since the ELXM-SW6 last saw a packet from this MAC address (device).
Hops	Displays the number of hops to a Master or AP device. A value of **na** (zero) appears for non-ProSoft Technology devices.

- This list contains both 802.11 devices that are part of the same SSID as the ELXM-SW6 (for example, *NetworkELXM*) as well as devices that belong to different SSIDs (for example, *Network11* and *fantree*). This list is updated continuously.
- The ELXM-SW6 updates this list with each 802.11 Beacon that is received, whether from a radio of the same network or one that belongs to another SSID. It can also see radios from other vendors.

3.3 Configuring Basic Settings

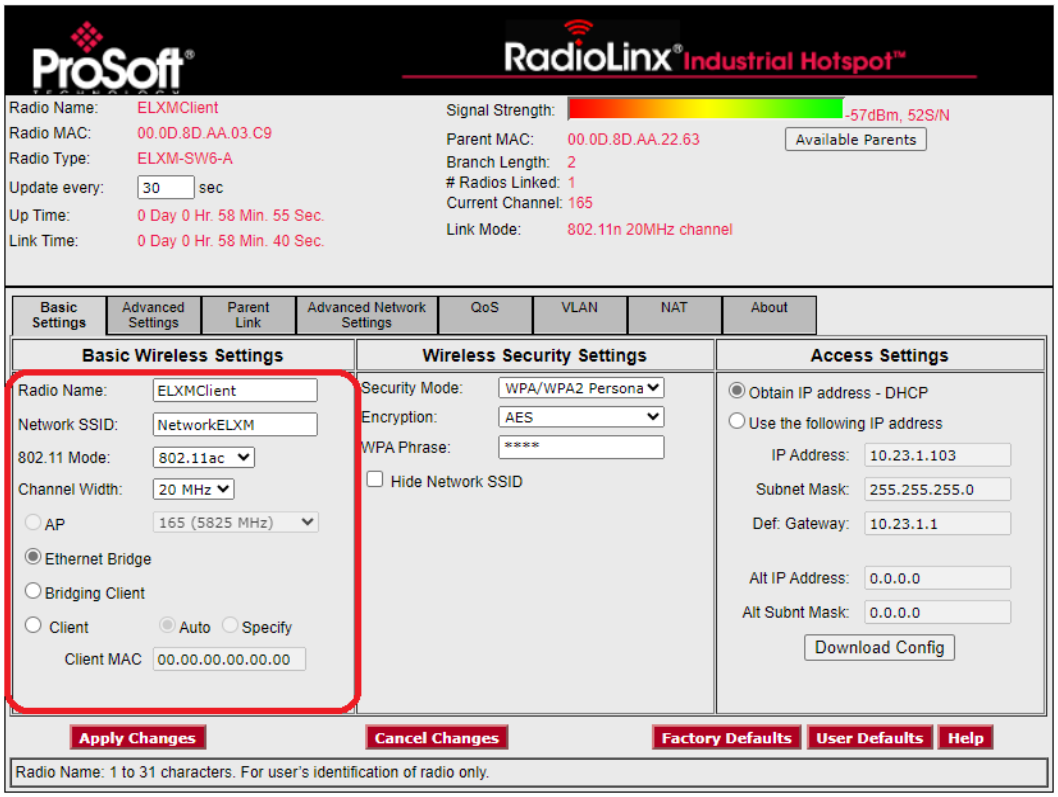
The **BASIC SETTINGS** tab includes three groups:

- **BASIC WIRELESS SETTINGS**
- **WIRELESS SECURITY SETTINGS**
- **ACCESS SETTINGS**



3.3.1 Basic Wireless Settings

Use the parameters in the **BASIC WIRELESS SETTINGS** group to define the identity of the ELXM-SW6.



Note: Different versions of the ELXM-SW6 and firmware support different functions. There may be fewer or more parameters on this page, depending on the version of the ELXM-SW6 and firmware.

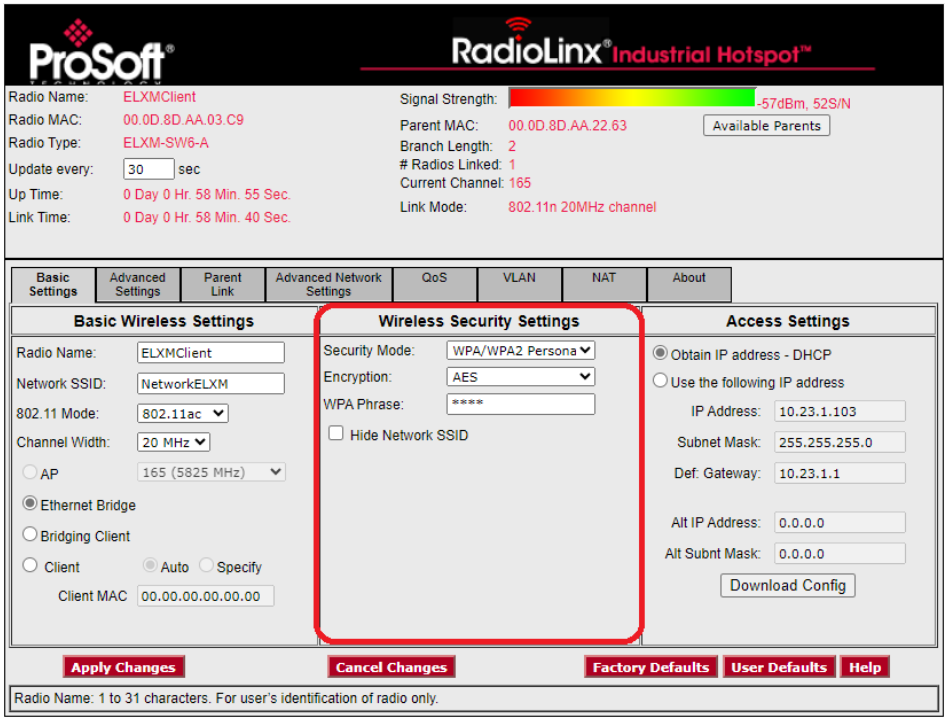
Parameter	Description
Radio Name	Specifies a unique name for the ELXM-SW6 to be configured.
Network SSID	Specifies a network name (SSID) of up to 32 characters and defines the network that the ELXM-SW6 will join and be part of. All radios with this SSID are part of the same network. **Note:** SSID names are case-sensitive.

Parameter	Description
802.11 Mode	Specifies the version of the 802.11 standard that will be used by the ELXM-SW6. **Note:** The ELXM-SW6 automatically uses a mode that is compatible with the Parent radio. For example, an ELXM-SW6 may connect to an RLX2-IHNF Master radio which only operates in 802.11a/g/n mode. **802.11A/G -** The ELXM-SW6 acts as an 802.11a radio on the 5 GHz band, and an 802.11g radio on the 2.4 GHz band. Data rates are limited to the 802.11 a/g rates (54 mbps maximum, and. 802.11n/ac/ax operational features are disabled. It is **not** necessary to select this mode for the ELXM-SW6 to link to APs that only support 802.11a/g. These radios link at their best possible speeds regardless of mode. This mode is not commonly used. It is mainly used to force operation at 802.11a/g rates due to environmental or compatibility issues, if needed. The 802.11a/g mode only supports 20 MHz channels. **802.11N -** All 802.11n features are operational, and the ELXM-SW6 uses 20 MHz or 40 MHz wide channels as set by the Channel Width control. **802.11AC -** All 802.11ac features are operational, and the ELXM-SW6 uses 20 MHz, 40 MHz or 80 MHz wide channels as set by the Channel Width control. **802.11AX -** All 802.11ax features are operational, and the ELXM-SW6 uses 20 MHz, 40 MHz or 80 MHz wide channels as set by the Channel Width control.
Channel Width	Specifies the width of the channel the ELXM-SW6 will use when transmitting. **20 MHz:** The default bandwidth supported by all 802.11 modes. **40 MHz:** Utilizes adjacent pairs of 20 MHz-wide channels as a single 40 MHz-wide channel. This allows faster data throughput to other 802.11 devices. This bandwidth is supported by 802.11n/ac/ax devices, but all ELXM-SW6's will only transmit at this channel width if it is supported by a peer radio. Channels in the 5 GHz band are 20 MHz apart, so 40 MHz channel width occupies only two channels in that band. However, channels in the 2.4 GHz band are spaced only five MHz apart; this width occupies *eight adjacent channels.* **80 MHz:** Utilizes four adjacent 20 MHz-wide channels as a single 80 MHz-wide channel. This allows the fastest data throughput to other 802.11 devices. This bandwidth is supported by 802.11ac/ax devices, but all ELXM-SW6's will only transmit at this channel width if it is supported by a peer radio. **Note:** Although this channel width provides the highest data rates, it is also more susceptible to interference from other sources utilizing parts of the 80MHz channel. Therefore, the use of 80 MHz channels is not recommended in most industrial and enterprise environments where there are many different wireless networks operating in near proximity on all available 20 MHz channels.

Parameter	Description
AP	Access Point specifies the ELXM-SW6 will operate as an 802.11 AP. The AP is the root device in a network. At least one AP must be in the network. For redundancy, assign more than one AP to a network. **Note:** AP mode may not be enabled in some early versions of ELXM-SW6 firmware.
Available Channel List (For AP only)	Specifies the channel number, the frequency band (2.4 GHz, 5 GHz DFS, or 5 GHz), and the channel frequency in MHz. **For ELXM-SW6's:** When **CHANNEL WIDTH** is set to **40 MHz**, each entry shows the main channel number, followed by the extension channel number if the channel supports 40 MHz. The 20 MHz channels are used whenever sending frames at an 802.11 a/g data rate (for example, Beacons at 6 Mbits). The main and extension channels are used together for 802.11n/ac/ax data rate transmissions. Note that the frequency indicated when the Channel Width is set to 40 MHz is the center of the 40 MHz channel pair. **Important:** The ELXM-SW6 is not supplied with an antenna. Select an antenna that supports the frequency range set in the configuration for the ELXM-SW6.
Ethernet Bridge	Specifies that the ELXM-SW6 is in a Client mode that should only be used when all radios in the network (SSID) are ProSoft Technology radios. In this mode all Ethernet data packets are bridged at layer 2 between the ELXM-SW6 client and the ProSoft Technology AP. **Note:** Ethernet Bridge mode is not compatible with 3rd Party Access Points (APs).
Bridging Client	Specifies a special mode for use where there are multiple Ethernet devices that need to connect to any 3rd-party 802.11 Access Points (AP). This mode uses a Layer 2 Network Address Translation mechanism and can only work for IP-based protocols. If using non-IP-based protocols, then specify Client mode for the ELXM-SW6. For more information, see section *2.5.3 Configuring as a Bridging Client Radio*.
Client	This is a special mode that allows you to transparently connect a single Ethernet device to any non-ProSoft Technology 802.11 Access Point (AP). To the AP, the MAC address of the Ethernet device would appear to be an 802.11 wireless client. Client mode supports all network protocols. For more information, see section *2.5.4 Configuring as a Client Radio*.
Auto / Specify (Client mode only)	Choose **SPECIFY** only if the device does not send out any unsolicited Ethernet packets. Try **AUTO** first.
Client MAC	Specify the MAC ID of the device connected to the ELXM-SW6, only if the device does not advertise its MAC address.

3.3.2 Wireless Security Settings

Use the parameters in the **WIRELESS SECURITY SETTINGS** group to define the wireless security parameters for the ELXM-SW6.



The parameters in the *Wireless Security Settings* depend on the selections in the following parameters:

- **SECURITY MODE**
- **802.11 MODE**
- **AP**, **ETHERNET BRIDGE**, **BRIDGING CLIENT**, or **CLIENT** radio modes

The parameters in the *Wireless Security Settings* group automatically change when these parameters are edited. Clicking **APPLY CHANGES** is not necessary to see the changes in the *Wireless Security Settings*.

Parameter	Description
Security Mode	Specifies the security mode for the ELXM-SW6, as well as Legacy WEP encryption modes for interoperability with Legacy devices. **NONE:** (not recommended) **PERSONAL:** Security mode using a pre-shared key for networks that don't require an authentication server. **ENTERPRISE:** Security mode requiring the use of an external RADIUS authentication server. For more information see section *3.3.2.2 Enterprise Mode Settings*. The following protocols are available with both Personal and Enterprise security modes: **WPA:** Original protocol introduced to replace WEP. **WPA2:** 802.11 security protocol conforming to the 802.11i standard. **WPA/WPA2:** Allows client devices to connect using WPA if they do not support WPA2.
Encryption	Specifies the encryption method for the ELXM-SW6. AES is the preferred encryption mechanism as it is the most secure protocol supported by the 802.11 standard. If using legacy devices that do not support AES, you can choose combinations of legacy methods depending on the 802.11 mode setting. **NONE:** (Not recommended) **AES:** (Recommended) This can be used with all Personal and Enterprise modes. **TKIP:** Only TKIP encryption. This setting is only available when in 802.11a/g mode. The 802.11n and newer standards do not allow TKIP as the only encryption mechanism. **AES AND TKIP:** Allows client devices that do not support AES to connect to the ELXM-SW6. This setting is available in all 802.11 modes. For more information, see section *3.3.2.1 Encryption Type*.
WPA phrase	Specifies the WPA pass phrase of between eight and 63 normal keyboard characters. This control is present when you select any of the **PERSONAL** Security Modes. If a **WPA** or **WPA2** Personal Security Mode is selected, enter a WPA phrase of between eight and 63 normal keyboard characters. As an aid to creating a secure pass phrase the background color of the edit field will change from red to yellow to light green to dark green depending on length of passphrase and whether the characters entered contain a mix of lower case, upper case, special characters, and numbers. Ensure that the pass phrase selected is highlighted with a dark green background. This phrase automatically generates an encryption key of 128 hexadecimal characters. The default WPA Phrase is **passphrase**
Hide Network SSID	Select this check box to hide the **NETWORK SSID** (defined in the *Basic Wireless Settings* group) from other 802.11 users. Clients can still connect to the radio network by manually entering the Network SSID.

3.3.2.1 Encryption Type

It is recommended to use WPA or WPA2 (Wi-Fi Protected Access) using AES for the **SECURITY MODE** and **ENCRYPTION**. Use TKIP with an older client radio that does not support AES.

Important: If the 802.11n/ac/ax data rates are enabled in the ELXM-SW6, then all TKIP options are disabled. If the peer radio only supports TKIP, then use the **AES AND TKIP** option.

3.3.2.2 Enterprise Mode Settings

When one of the **ENTERPRISE** modes is selected in the *Security Mode* control of the *Wireless Security Settings* group, the webpage automatically displays a set of controls for Enterprise mode parameters. There are two sets of controls:

- The first set is for the ELXM-SW6 in AP mode
- The second set is for the ELXM-SW6 in Bridge or Client mode.

3.4 Enterprise security parameters in AP mode

In **ENTERPRISE** mode, the ELXM-SW6 authenticator communicates directly with the RADIUS Server while it is relaying 802.1x frames received from an associating note's Supplicant. Configure the following parameters in the *Wireless Security Settings* group on the Master radio in this *Security Mode*:

Parameter	Description
IP Address	Specifies the IP address of the RADIUS server with which the Network Administrator has registered the ELXM-SW6.
UDP Port	Specifies the UDP port number the RADIUS server is using to listen to Radius frames from the ELXM-SW6. The default port number used for the Radius protocol is 1812.
Secret	Specifies the pass phrase that was used when the ELXM-SW6 was registered to the RADIUS server. This validates that the Radius frames received on either end are legitimate.

3.5 Enterprise security parameters in Bridge or Client modes

When in Bridge or Client mode, the ELXM-SW6 Supplicant communicates via its Parent radio's authenticator with a RADIUS server. Several different authentication protocols are available and can be set using the following parameters.

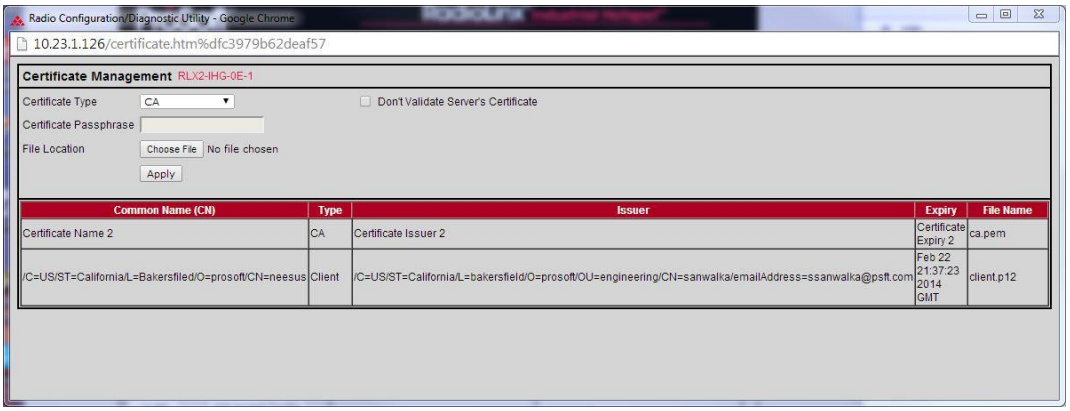
Parameter	Description
EAP Method	Specifies the EAP Method, sometimes referred to as the 'outer protocol' defines the mechanism used to create a secure tunnel between the Supplicant and RADIUS server during the first phase of the Authentication sequence. The following EAP methods are supported: **EAP-PEAP:** EAP method using the Protected Extensible Authentication Protocol. **EAP-TLS:** EAP method based on X.509 certificates that provides for mutual authentication. This is the most secure authentication mechanism available for 802.11. Certificates are required both on the ELXM-SW6 and the RADIUS server. The only authentication option available for EAP-TLS is to use TLS for the inner protocol. **EAP-TTLS:** EAP Tunneled TLS. Similar to EAP-PEAP.
Anonymous ID	Specifies the identity request in the first phase of the exchange that is sent in the clear when using **EAP-PEAP** or **EAP-TTLS**. The identity sent in this first phase can be set to an anonymous identity (for example *anon_user*) or an anonymous identity at a domain (for example anon@xyz.com). The real identity (*username*) is sent encrypted after the EAP tunnel is established in the second phase of the radius exchange. Use this parameter if you are concerned about the username being sent in the clear. Your IT department should specify the text for this parameter based on their RADIUS server(s) configuration.
Authentication Method	Specifies the authentication method, sometimes referred to as the inner protocol. This defines the mechanism used to authenticate the Supplicant of the ELXM-SW6 with the RADIUS server. The following authentication methods are supported: **MS-CHAPv2:** Microsoft's version of the Challenge Handshake Authentication Protocol. This method provides mutual authentication between the Supplicant and the RADIUS server, using a username and password and challenge text responses. **TLS:** Certificate-based inner authentication protocol.
Username	Specifies the username of the account that is to be authenticated. When using EAP-TLS, this represents the identity of the entity assigned to the device certificate being used.
Password	Specifies the required password when using **EAP-PEAP** or **EAP-TTLS** with **MS-CHAPv2**. This is the password of the account corresponding to the **USER NAME**.
Certificates	Displays the current certificates installed in the ELXM-SW6 and provides controls to upload new certificates into the ELXM-SW6. For more information, see section *3.5.1 Certificate Management*. **Note:** The ELXM-SW6 does not ship with any certificates installed.

3.5.1 Certificate Management

When using Enterprise-level security, some EAP methods require the use of X.509 certificates that you must upload to the ELXM-SW6. There are two certificate types: (1) a certificate from a 'Certification Authority' used to authenticate the RADIUS server to the ELXM-SW6 supplicant, and (2) device or client certificate created by the RADIUS server for the ELXM-SW6. The ELXM-SW6 is can hold one of each certificate type.

- If using EAP-PEAP authentication, a CA Certificate (to authenticate the RADIUS server) is needed.
- If using EAP-TLS, a CA Certificate, a .p12 file that contains both the Client Certificate, and the Private Key needed to authenticate the client are needed. The p12 file is encrypted and requires a password.
- Check with the IT Department to provide the appropriate files needed to load to the ELXM-SW6 Client radio.

1 Obtain the required certificate files from the IT department.
2 Log into the ELXM-SW6.
3 Click the **BASIC SETTINGS** tab, then in the *Wireless Security Settings* group, select the **EAP METHOD**.
4 Enter the **USERNAME**.
5 Click **CERTIFICATES**. This displays the *Certificate Management* dialog to enter the certificate files.



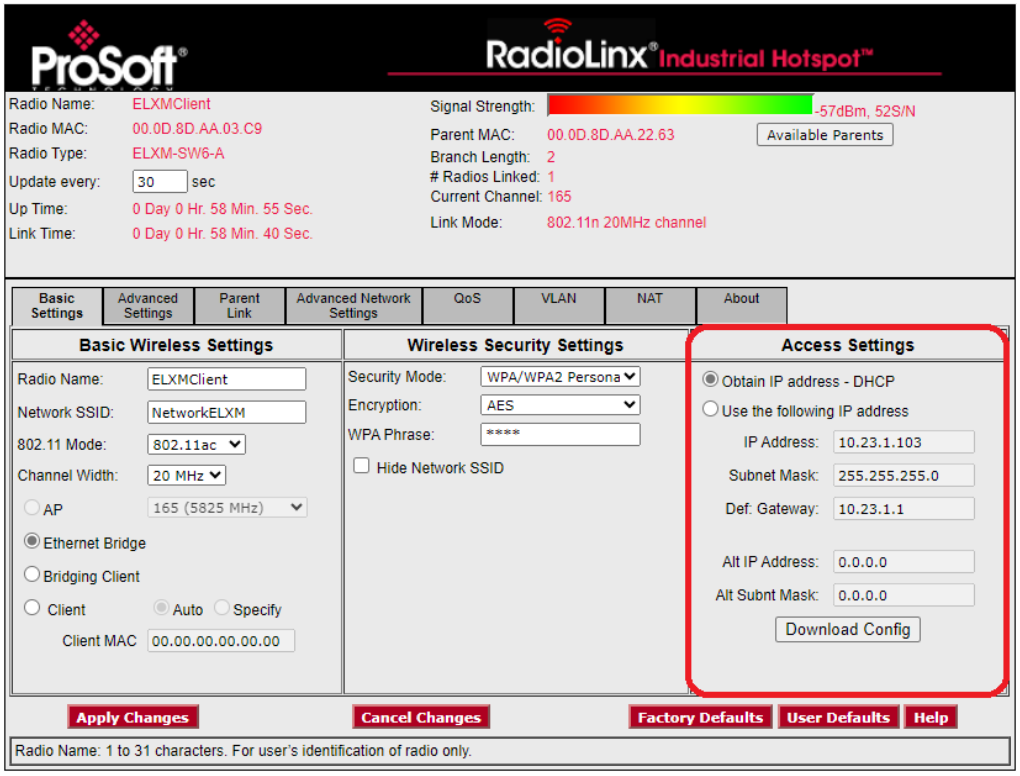
Parameter	Description
Certificate Type	Specifies the type of certificate that you are uploading. It is important that this is set correctly as the ELXM-SW6 does not distinguish between certificate types in any other way. A CA Certificate is required for both PEAP and EAP-TLS. This is used to authenticate the server's certificate. Additionally, for EAP-TLS, a client certificate and private key are required.
Certificate Passphrase	If the certificate is encrypted, enter the passphrase that was used to create it on the RADIUS server.
File Location	Selects the certificate file on your local PC that to be uploaded.
Don't Validate Server's Certificate	The ELXM-SW6 does not validate the server's certificate.

6 Select the **CERTIFICATE TYPE**.

7 Click **CHOOSE FILE** to select the CA Certificate file created previously (CAcert.pem) and click **APPLY**.
8 Click **CHOOSE FILE** to select the Client Certificate combined file (clientcert.p12) and the password associated with the file, and then click **APPLY**.
9 Close the *Certificate Management* dialog box.
10 In the main window, click **APPLY CHANGES** and attempt to connect to the Master radio.

3.5.2 Access Settings

Use the parameters in the *Access Settings* group to define how the ELXM-SW6 gets an IP address.



Parameter	Description
Obtain IP Address -DHCP	Select this if the ELXM-SW6 is to automatically get an IP address through DHCP
Use the following IP address	Select this to manually define IP address for the ELXM-SW6. Enter the IP address information in the remaining parameters.
IP Address	Specifies the unique IP address assigned to the module
Netmask	Specifies the subnet mask of module
Def. Gateway	Specifies the network gateway (if used)
Alt IP Address	Specifies a 2nd IP Address for the module to be used with VLANs
Alt Subnet Mask	Specifies the subnet mask for the 2nd IP Address
Download Config button	Downloads the current ELXM-SW6 configuration from the radio to the PC/laptop. For more information, see section *3.1.6.1 Uploading User Defaults to an* ELXM-SW6.

1. On the **BASIC SETTINGS** tab, in the *Access Settings* group, click **OBTAIN IP ADDRESS - DHCP** or **USE THE FOLLOWING IP ADDRESS**.
2. If **USE THE FOLLOWING IP ADDRESS** is selected, enter the information for the IP address.
3. Click **APPLY CHANGES** to reboot the ELXM-SW6.

3.6 Configuring Advanced Settings

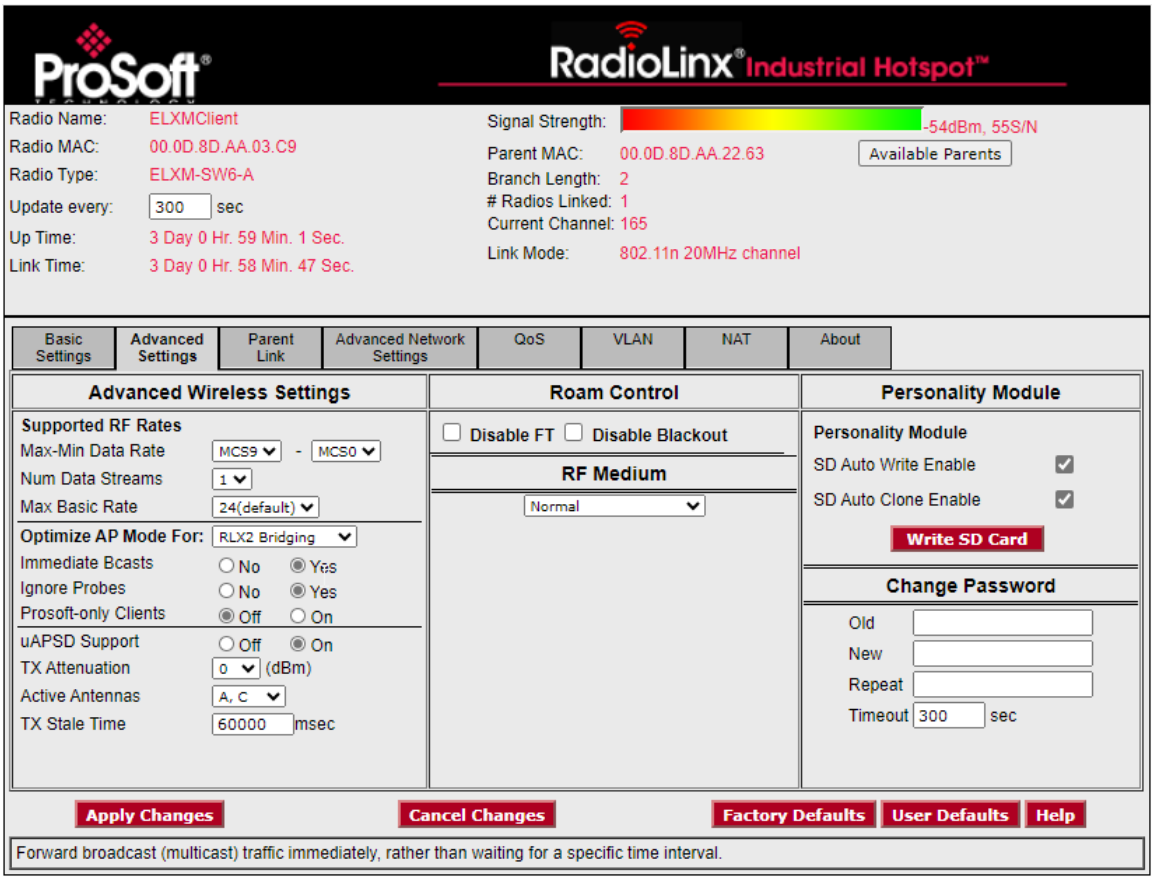
It is important to allow many industrial protocols to communicate properly through the ELXM-SW6's. The standard 802.11 AP operation for transmitting broadcast messages is to accumulate them and transmit them on specific time intervals. This allows clients that are in power-save mode to wake up at the synchronized time interval and receive the broadcast packets. However, the power-save mode is rarely used in industrial networks.

Additionally, many industrial protocols utilize multicast traffic, which is sent as broadcast messages over the wireless network. By enabling immediate broadcasting, these multicast messages are not delayed by waiting for the next time interval to occur. This results in improved network performance.

The settings allows the configuration of the transmission rate and broadcast mode to optimize the ELXM-SW6's use on an industrial network.

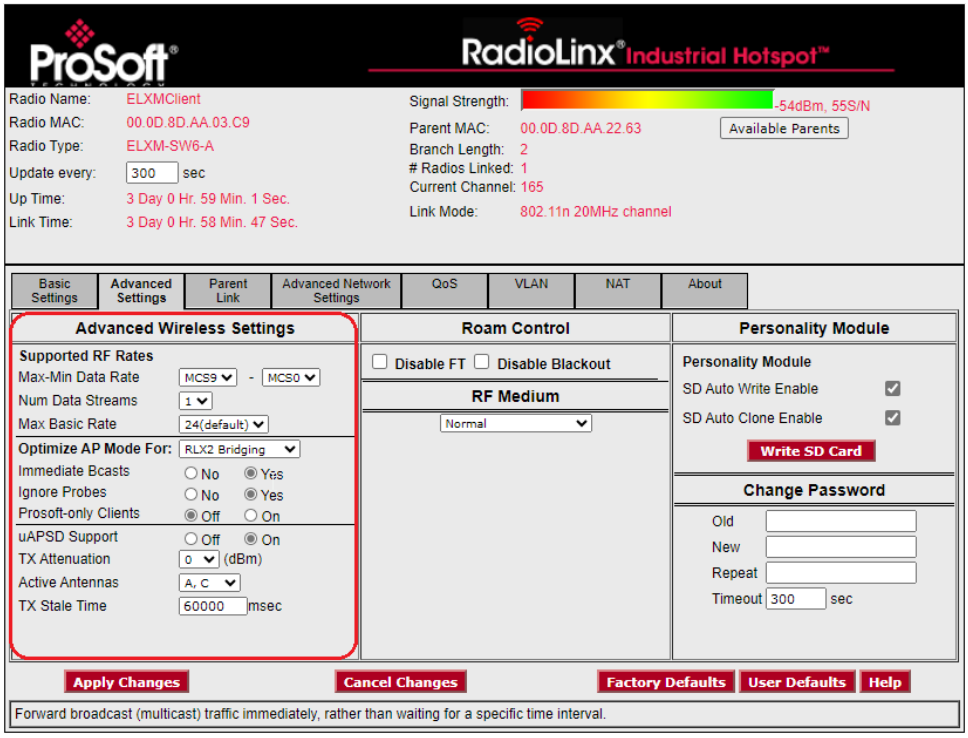
Advanced Settings include:

- Advanced Wireless Settings
- Roam Control
- RF Medium
- Personality Module
- Change Password



3.6.1 Advanced Wireless Settings

Use the parameters in the *Advanced Wireless Settings* group to specify the wireless communication parameters of the ELXM-SW6.



It is important to allow many industrial protocols to communicate properly through the ELXM-SW6's.

The standard 802.11 AP operation for transmitting broadcast messages is to accumulate them and then transmit them only on specific time intervals. This allows clients in power-save mode to wake up at the specified time interval and receive the broadcast packets.

However, power-save mode is rarely used in industrial networks. Additionally, many industrial protocols use multicast traffic which is sent as broadcast messages over the wireless network.

By enabling immediate broadcasting, these multicast messages are not delayed by the wait for the next time interval to occur before they are transmitted. This results in improved network performance.

The settings on this form allow the configuration of the transmission rate and broadcast mode to optimize the ELXM-SW6's use of an industrial network.

Parameter	Description
Min-Max Data Rate	In AP Mode, the maximum and minimum data transmission rates, advertised by the ELXM-SW6 in its Beacon. All wireless devices connected to the ELXM-SW6 will limit their Tx Rate to values in this range. Available settings range from: • 1 to 54 when in 802.11a/g mode • MCS0 to MCS7 when in 802.11n mode with only 1 data stream • MCS0 to MCS15 when in 802.11n mode with 2 data streams • MCS0 to MCS9 when in 802.11ac mode • MCS0 to MCS11 when in 802.11ax mode Note that in 802.11n mode, data rates MCS0 – MCS7 are independent of the number of stream, whereas in 802.11ac/ax the data MCS data rates double when 2 streams are enabled.
Num Data Streams	The number of data streams that will be transmitted simultaneously when sending a wireless packet. Using 2 data streams doubles the bit rate on the air. In general, using a single stream is preferred in industrial networks if the single stream bit rates are sufficient for the application. The higher 2 stream data rates require higher signal to noise ratios and are more susceptible to multipath and interference.
Max Basic Rate	The maximum Basic transmission rate, advertised by the ELXM-SW6 in its Beacon. Basic Rates are used for packets such as Broadcasts that need to go to the whole network and for Management frames. The Max Basic Rate setting of the AP is advertised to each of the radios in the network through Beacons. Each radio, other than the AP, then inherits the Max Basic Rate setting of the AP. Therefore, the setting only needs to be made in the AP radio. The setting in each of the other radios is disregarded. Available settings range from 1 to 54 Mb/s.
Optimize For	This control allows ease of configuration for the *Immediate Bcasts*, *Ignore Probes* and Prosoft Technology-only Client controls, for three specific interoperability scenarios when operating in AP mode: **3RD PARTY CLIENTS:** Optimizes these controls to provide an infrastructure for peer devices such as laptops, tablets, phones, or any other Wi-Fi devices that perform regular power saving. If this setting is not used, then these client devices may have difficulty in finding the network's SSID, and their communication may be erratic due to broadcasts not being transmitted when expected. Bridging to ELXM-SW6 clients will still function although delivery of broadcast packets will be delayed. **ELXM-SW6 BRIDGING:** Optimizes Immediate Broadcasts, Ignore Probes and Range for operation when peer devices are primarily other ELXM-SW6s. **SECURE BRIDGING:** Similar to ELXM-SW6 Bridging but in addition enables the ProSoft-only Clients control which rejects any connections from 3rd-party client devices.
Immediate Bcasts	Specifies that the ELXM-SW6 forwards broadcast/multicast traffic immediately, rather than waiting for specific time intervals.
Ignore Probes	If set to **No** will respond to all Probe Requests that are received. If set to **Yes** will only respond to probe requests that are specific to the ELXM-SW6's SSID and will ignore all general probes.
ProSoft-only Clients	If set to **Off** will allow all 802.11 devices that have the correct security keys to connect to this Bridge. If set to **On**, will reject all connections from 3rd-party non-ProSoft wireless devices.

Parameter	Description
uAPSD Support	This determines whether uAPSD support (Unscheduled Automatic Power Save Delivery) is advertised in the ELXM-SW6's Beacons. When set to **Off**, client devices connecting to the ELXM-SW6 will not attempt to use uAPSD. When set to **On**, client devices will use uAPSD if they support it, otherwise they will use normal 802.11 power saving. uAPSD support is **On** by default. Typically, this would only be set to **Off** if the client device's implementation of uAPSD is not optimal and performance suffers when it attempts to use it. In these cases, response of the client device is often better when normal power saving is used.
TX Attenuation	This determines the amount of attenuation that will be applied to the output power of the ELXM-SW6. Mainly used when high gain antennas are used that would exceed the max Tx power allowed by the local regulatory body for the region the ELXM-SW6 will be installed
Active Antennas	This determines which of the ELXM-SW6's antenna ports are active. This control must be set to match the number of antennas that are installed. Note that 2 antennas are needed to achieve 2 stream data rates.
Tx Stale Time	Packets queued for transmission will be discarded if they have not been transmitted in the time set by this control. The main purpose of this control is to limit the duration of any congestion peaks that may occur on a channel that has high utilization. In industrial networks most data packets are time sensitive and if they do not arrive by a certain time are treated as if they were lost. Transmitting these packets after such a timeout would serve no purpose and simply adds load to the radio channel. On a busy channel any burst of interference or sudden unwanted load, such as a burst of broadcast traffic, may lead to large Tx latency times if the channel becomes saturated. Continuing to transmit stale data packets prolongs this condition even though the packets have already been treated as if lost by their destination. The default of this control is also the max value of 60,000 msec. The minimum allowed is 10 msec. This control should only be modified from its default if the packet load in aggregate on a channel is close to saturating the channel and set to a value that is greater than the max timeout value for any application connection.

3.6.1.1 802.11n Data Rates

			802.11n 20MHz, Mbit/s		802.11n 40MHz, Mbit/s	
MCS Index	**Active Antennas**	**# Streams**	**800 ns GI**	**400 ns GI**	**800 ns GI**	**400 ns GI**
0	1 or 2	1	6.5	7.2	13.5	15.0
1	1 or 2	1	13.0	14.4	27.0	30.0
2	1 or 2	1	19.5	21.7	40.5	45.0
3	1 or 2	1	26.0	28.9	54.0	60.0
4	1 or 2	1	39.0	43.3	81.0	90.0
5	1 or 2	1	52.0	57.8	108.0	120.0
6	1 or 2	1	58.5	65.0	121.5	135.0
7	1 or 2	1	65.0	72.2	135.0	150.0
8	2	2	13.0	14.4	27.0	30.0
9	2	2	26.0	28.9	54.0	60.0
10	2	2	39.0	43.3	81.0	90.0
11	2	2	52.0	57.8	108.0	120.0
12	2	2	78.0	86.7	162.0	180.0
13	2	2	104.0	115.6	216.0	240.0
14	2	2	117.0	130.0	243.0	270.0
15	2	2	130.0	144.4	270.0	300.0

3.6.1.2 802.11ac Data Rates

			802.11ac 20MHz, Mbit/s		802.11ac 40MHz, Mbit/s		802.11ac 80MHz, Mbit/s	
MCS Index	**Active Antennas**	**# Streams**	**800 ns GI**	**400 ns GI**	**800 ns GI**	**400 ns GI**	**800 ns GI**	**400 ns GI**
0	1 or 2	1	6.5	7.2	13.5	15.0	29.3	32.5
1	1 or 2	1	13.0	14.4	27.0	30.0	58.5	65.0
2	1 or 2	1	19.5	21.7	40.5	45.0	87.8	97.5
3	1 or 2	1	26.0	28.9	54.0	60.0	117.0	130.0
4	1 or 2	1	39.0	43.3	81.0	90.0	175.5	195.0
5	1 or 2	1	52.0	57.8	108.0	120.0	234.0	260.0
6	1 or 2	1	58.5	65.0	121.5	135.0	263.3	292.5
7	1 or 2	1	65.0	72.2	135.0	150.0	292.5	325.0
8	1 or 2	1	78.0	86.7	162.0	180.0	351.0	390.0
9	1 or 2	1	n/a	n/a	180.0	200.0	390.0	433.3
0	2	2	13.0	14.4	27.0	30.0	58.5	65.0
1	2	2	26.0	28.9	54.0	60.0	117.0	130.0
2	2	2	39.0	43.3	81.0	90.0	175.5	195.0
3	2	2	52.0	57.8	108.0	120.0	234.0	260.0
4	2	2	78.0	86.7	162.0	180.0	351.0	390.0
5	2	2	104.0	115.6	216.0	240.0	468.0	520.0
6	2	2	117.0	130.0	243.0	270.0	526.5	585.0
7	2	2	130.0	144.4	270.0	300.0	585.0	650.0
8	2	2	156.0	173.3	324.0	360.0	702.0	780.0
9	2	2	n/a	n/a	360.0	400.0	780.0	866.7

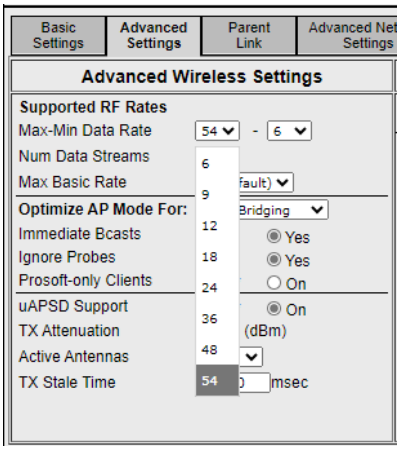
3.6.1.3 802.11aX Data Rates

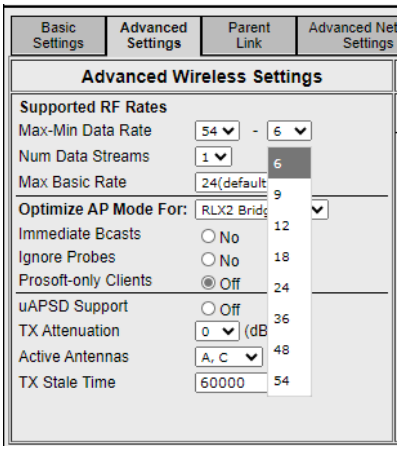
			242-tone RU-20MHz Mbits/s			484-tone RU-40MHz Mbits/s			996-tone RU-80MHz Mbits/s		
MCS Index	Active Antennas	# Streams	3200 ns GI	1600 ns GI	800 ns GI	3200 ns GI	1600 ns GI	800 ns GI	3200 ns GI	1600 ns GI	800 ns GI
0	1 or 2	1	7.3	8.1	8.6	14.6	16.3	17.2	30.6	34.0	36.0
1	1 or 2	1	14.6	16.3	17.2	29.3	32.5	34.4	61.3	68.1	72.1
2	1 or 2	1	21.9	24.4	25.8	43.9	48.8	51.6	91.9	102.1	108.1
3	1 or 2	1	29.3	32.5	34.4	58.5	65.0	68.8	122.5	136.1	144.1
4	1 or 2	1	43.9	48.8	51.6	87.8	97.5	103.2	183.8	204.2	216.2
5	1 or 2	1	58.5	65.0	68.8	117.0	130.0	137.6	245.0	272.2	288.2
6	1 or 2	1	65.8	73.1	77.4	131.6	146.3	154.9	275.6	306.3	324.3
7	1 or 2	1	73.1	81.3	86.0	146.3	162.5	172.1	306.3	340.3	360.3
8	1 or 2	1	87.8	97.5	103.2	175.5	195.0	206.5	367.5	408.3	432.4
9	1 or 2	1	97.5	108.3	114.7	195.0	216.7	229.4	408.3	453.7	480.4
10	1 or 2	1	109.7	121.9	129.0	219.4	243.8	258.1	459.4	510.4	540.4
11	1 or 2	1	121.9	135.4	143.4	243.8	270.8	286.8	510.4	567.1	600.5
0	2	2	14.6	16.3	17.2	29.3	32.5	34.4	61.3	68.1	72.1
1	2	2	29.3	32.5	34.4	58.5	65.0	68.8	122.5	136.1	144.1
2	2	2	43.9	48.8	51.6	87.8	97.5	103.2	183.8	204.2	216.2
3	2	2	58.5	65	68.8	117.0	130.0	137.6	245.0	272.2	288.2
4	2	2	87.8	97.5	103.2	175.5	195.0	206.5	367.5	408.3	432.4
5	2	2	117.0	130.0	137.6	234.0	260.0	275.3	490.0	544.4	576.5
6	2	2	131.6	146.3	154.9	263.3	292.5	309.7	551.3	612.5	648.5
7	2	2	146.3	162.5	172.1	292.5	325.0	344.1	612.5	680.6	720.6
8	2	2	175.5	195.0	206.5	351.0	390.0	412.9	735.0	816.7	864.7
9	2	2	195.0	216.7	229.4	390.0	433.3	458.8	816.7	907.4	960.8
10	2	2	219.4	243.8	258.1	438.8	487.5	516.2	918.8	1020.8	1080.9
11	2	2	243.8	270.8	286.8	487.5	541.7	573.5	1020.8	1134.3	1201.0

The ELXM-SW6 automatically selects the Guard Interval (GI) based on current operating conditions. The system attempts to use a smallest GI, but will fall back to a larger GI if excessive data corruption is detected. The user has no control of the GI.

When the ELXM-SW6 is in 802.11a/g mode:

Advanced Wireless Settings includes the following Data Rates:





3.6.1.4 Active Antennas: ELXM-SW6

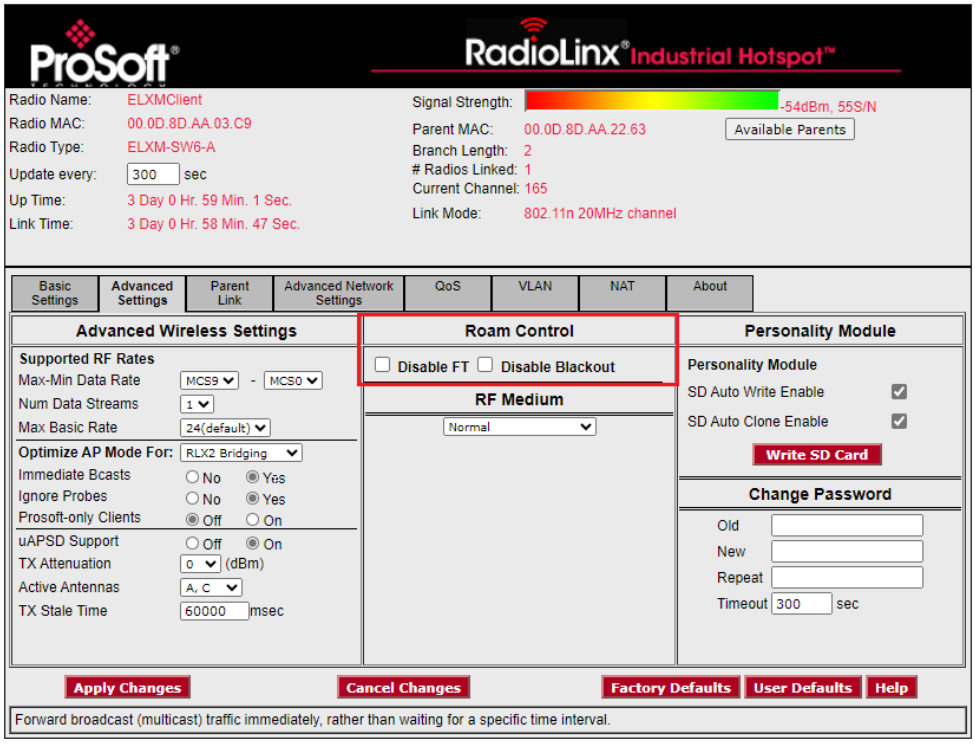
There are two options for the **ACTIVE ANTENNAS** parameter:

- **A, C** (the default setting; used for a two connector MIMO antenna).
- **A ONLY** for one SISO antenna

In general, using MIMO antennas gives the best performance.

3.6.2 Roam Control Settings

Use the parameters in the *Roam Control* group to specify the roaming wireless communication parameters of the ELXM-SW6.



In roaming applications, a mobile platform equipped with the ELXM-SW6 roams from one AP radio's coverage area to another radio's coverage area. By default, a Client radio roams automatically by calculating the cost for each roam candidate based only on RSSI and hop count. A lower cost determines when a better Parent radio candidate is present.

The ELXM-SW6 uses parts of the Fast Transition (FT) standard to reduce the time it takes to roam. An FT Roam will be used if the Client radio, the current Parent radio, and the next Parent radio all have FT enabled. *FT Roaming* can be disabled to use normal non-FT Roaming.

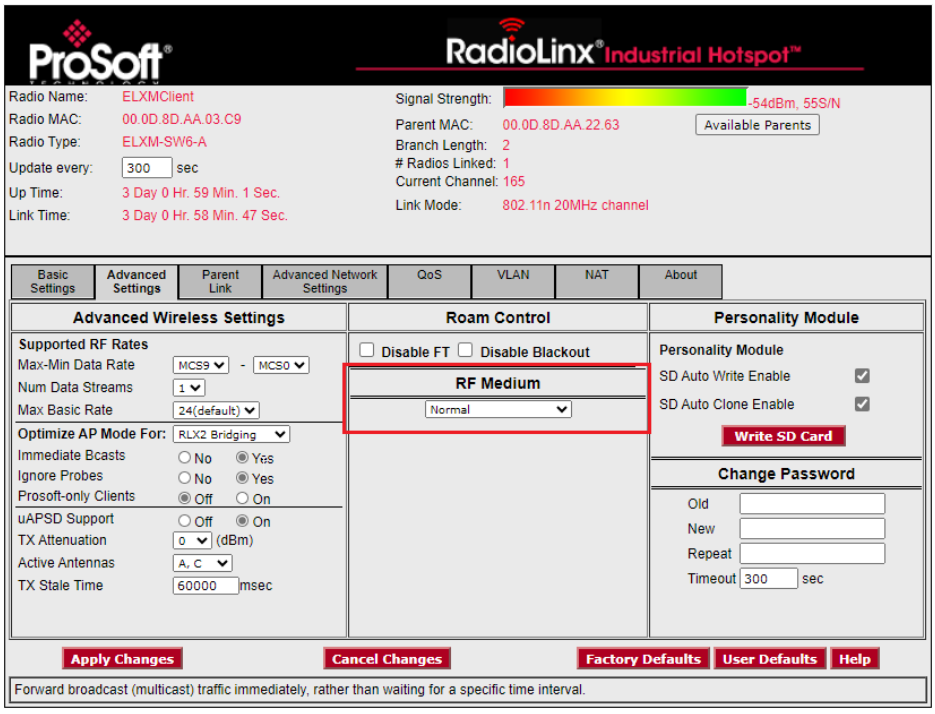
Parameter	Description
Disable FT	When checked this disables Fast Transition (FT) roaming in the ELXM-SW6. **Note:** With FT disabled, the roam duration could double and roams are no longer 'hitless' as there may be some frame loss in the Parent-to-Child direction. FT should be enabled other than a few exceptional circumstances. For example, if a 3rd party client device will not associate to the ELXM-SW6 because FT is enabled, or if the RSSI to the Parent is so low at a roam point that FT frames are lost during the roam.

Disable Blackout	When a Client's Parent Link is broken due to Sync Loss or if the initial connection fails for any reason a Blackout time is set to that Parent candidate so that the Parent selection algorithm will be forced to try another Parent even if its inferior. This works well when there are always other decent Parent candidates available. In some applications the physical setup is such that all other candidates in some locations are so weak, that any connection to them will be unusable. When it is known that there might only be one valid Parent candidate at times, this control when checked in the Client will allow the Parent selection algorithm to ignore any Blackout time that's been set to a Parent and allow an immediate reconnection attempt and prevent a lengthy connection outage. This control is disabled when in AP mode.

3.6.3 RF Medium Settings

This section contains the settings used to handle a roam across a medium discontinuity that would normally result in either packet loss or a disconnect/connect sequence.

A special mode is used by the ELXM-SW6 Client. This mode requires the use of two separate antennas and can detect when the ELXM-SW6 is traversing such a discontinuity. It can trigger a roam to the next AP before the 2nd lagging antenna has reached the discontinuity.



Note: The default *RF Medium* setting is **Normal**. If set to **Discontinuous** mode it must be set on both AP and Client. In the Client, setting to Discontinuous mode will also automatically result in the following configuration changes:

* The *Active Antennas* will be set to 2 Active Antennas (A & C).

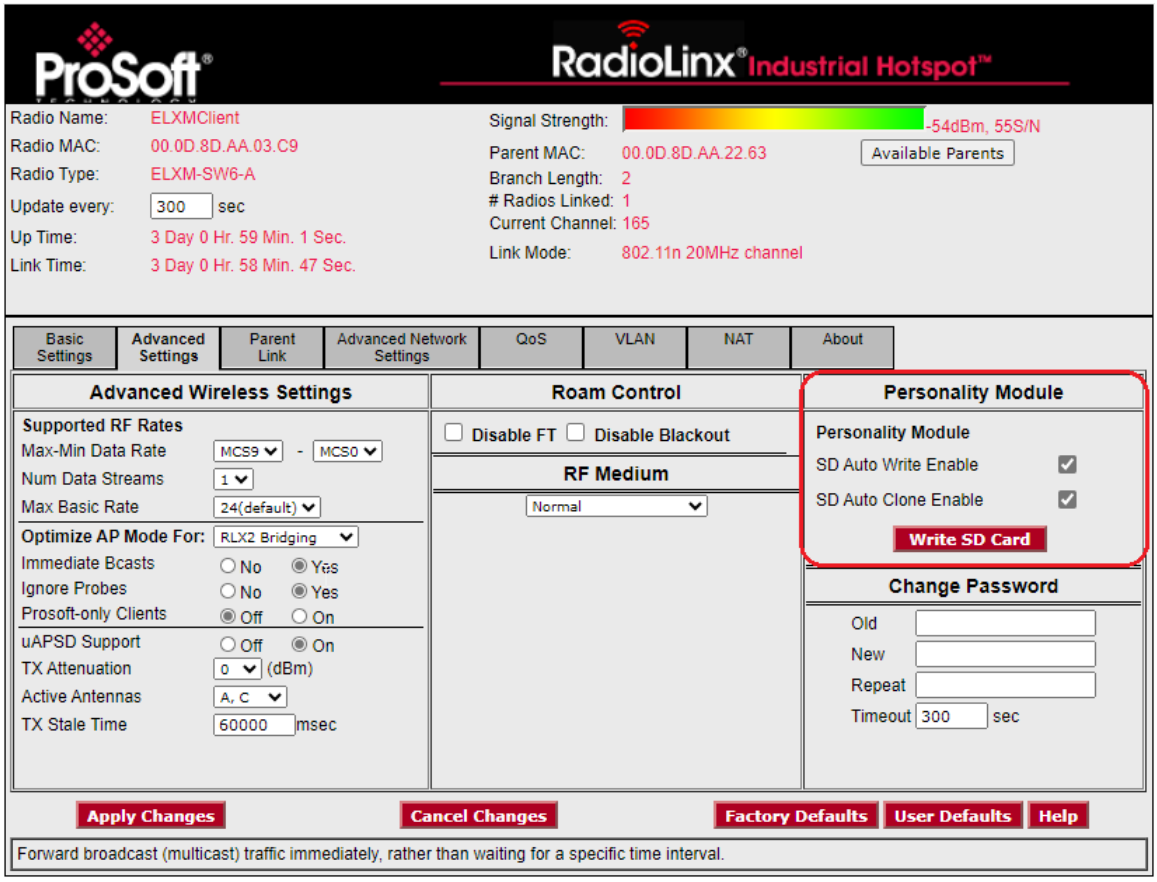
* The *Max Data Rate* will be set to the highest single stream MCS rate supported by the configured 802.11 mode, however the user is free to set a lower MCS rate. It will not allow 2 streams to be set.

* The *Min Data Rate* will be set to MCS0, a higher MCS rate can be set to less than the Max Data Rate.

Parameter		Description
Normal		Select when a continuous RF path exists when moving from one AP to another. This is typically the case when a MIMO or Omni antenna is attached to the ELXM-SW6 APs, or when using a continuous Radiating Cable or a Waveguide with an AP feeding each end.
Discontinuous		Select for applications where Radiating Cable or Waveguide segments from two adjacent APs are not joined, but instead independently terminated. This forms a small high RF loss gap between them. Transitioning from one segment to the next results in an abrupt discontinuity in RF Signal Strength to the current Parent, as the Client crosses the gap between segments.
	Minimum Transit Time (*Discontinuous* mode only)	Selects the minimum time in seconds it takes for both ELXM-SW6 antennas (A & C) to traverse across a segment discontinuity. This represents the maximum time available to roam from one segment to the next. Example: Assume the antennas are placed 2 meters apart and maximum speed is 1.2 m/s. Transit Time = 2m / 1.2m/s = 1.66 sec. Select the closest value that is smaller than 1.66 sec.
	Threshold (*Discontinuous* mode only)	Sets the minimum amount of change to the RF signal received on the leading antenna to indicate a segment discontinuity.

3.6.4 Personality Module Settings

Use the parameters in the *Personality Module* group to enable and disable the use of the microSD card (Personality Module) feature of the ELXM-SW6. Use the microSD card to save the ELXM-SW6's configuration. This makes it easy to replace the ELXM-SW6 with a new ELXM-SW6 by moving the microSD card from the old ELXM-SW6 to the replacement ELXM-SW6. For information, see section *2.7 Replacing an Existing ELXM-SW6*.

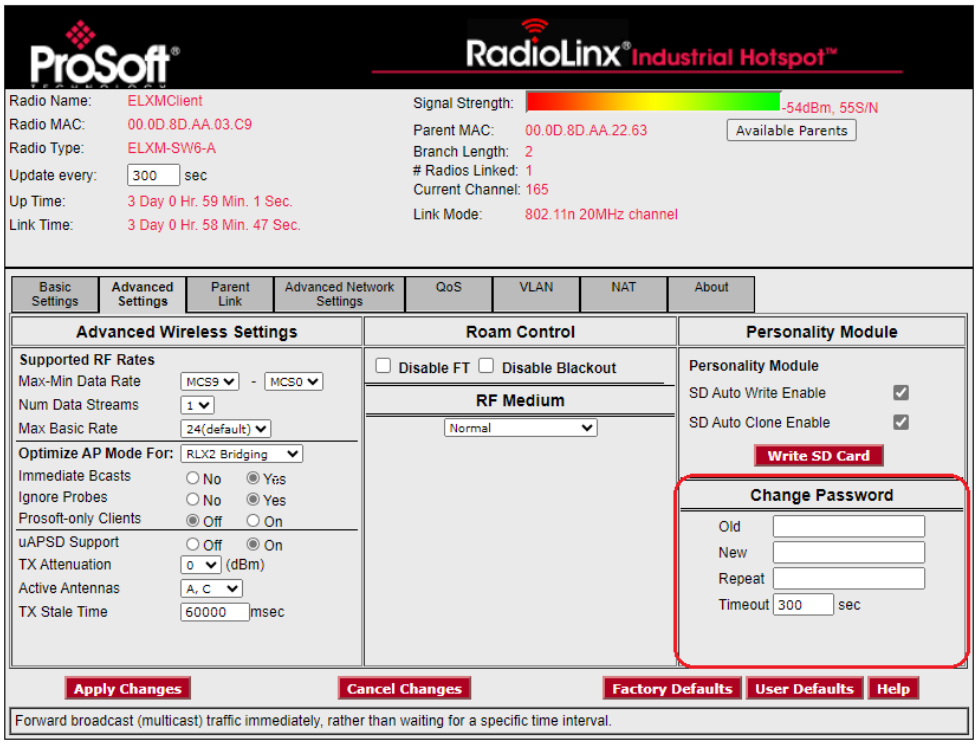


Note: The configuration files on the microSD card are stored in an encrypted binary format so sensitive data (e.g. passwords, encryption keys) cannot be read from the files.

Parameter	Description
SD Auto Write Enable	Select this check box to have the ELXM-SW6 write a copy of its configuration to the microSD whenever new settings are saved from the web configuration interface. The ELXM-SW6 renames previous configuration files with a unique file name that allows you to audit changes made to the ELXM-SW6's configuration.
SD Auto Clone Enable	Select this check box to have the ELXM-SW6 use the configuration from the microSD card when the ELXM-SW6 powers up. • If a microSD card is present and has a configuration file that is different from the ELXM-SW6's current configuration, the ELXM-SW6 uses the configuration from the microSD card. • If the configuration on the microSD card matches the ELXM-SW6's configuration, or there is no configuration file on the microSD card, then no action is taken. • If the microSD card is inserted into a running ELXM-SW6, and if the configuration file on the microSD is different from the ELXM-SW6's current configuration, the ELXM-SW6 gives a warning by flashing the **Signal Strength**, **MOD** and **NET** LEDs. If you reboot the ELXM-SW6 or cycle power, it uses the configuration from the microSD. To save this control as enabled (checked), either the microSD card slot in the ELXM-SW6 must be empty or enable the **SD AUTO WRITE ENABLE** control before saving. If these conditions are not present, the software disables this control before saving. This prevents the ELXM-SW6 from unintentionally reverting to a configuration file on the microSD card after resetting. • To use the configuration file on an SD card when this control is already enabled, insert the microSD and cycle power to the ELXM-SW6. • If this control is not enabled, enable it and save the setting without the microSD inserted (click **APPLY CHANGES**), then insert the microSD card, and then cycle power to the ELXM-SW6. **Note:** Do not enable **SD AUTO WRITE ENABLE** if you do not want the active configuration file on the microSD card to be replaced when the ELXM-SW6 loads and saves the microSD card's current configuration file.
Write SD Card	Immediately writes a copy of the ELXM-SW6's configuration file to the microSD card, independent of the **SD AUTO WRITE ENABLE** setting.

3.6.5 Changing Password Settings

Use the parameters in the *Change Password* group to change the password used to access the ELXM-SW6.



1. Enter the old password in **OLD**.
2. Enter the new password in **NEW**.
3. Enter the new password again in **REPEAT**.
4. Click **APPLY CHANGES**.

The **TIMEOUT** parameter sets the time before a login session is terminated at the ELXM-SW6's web server.

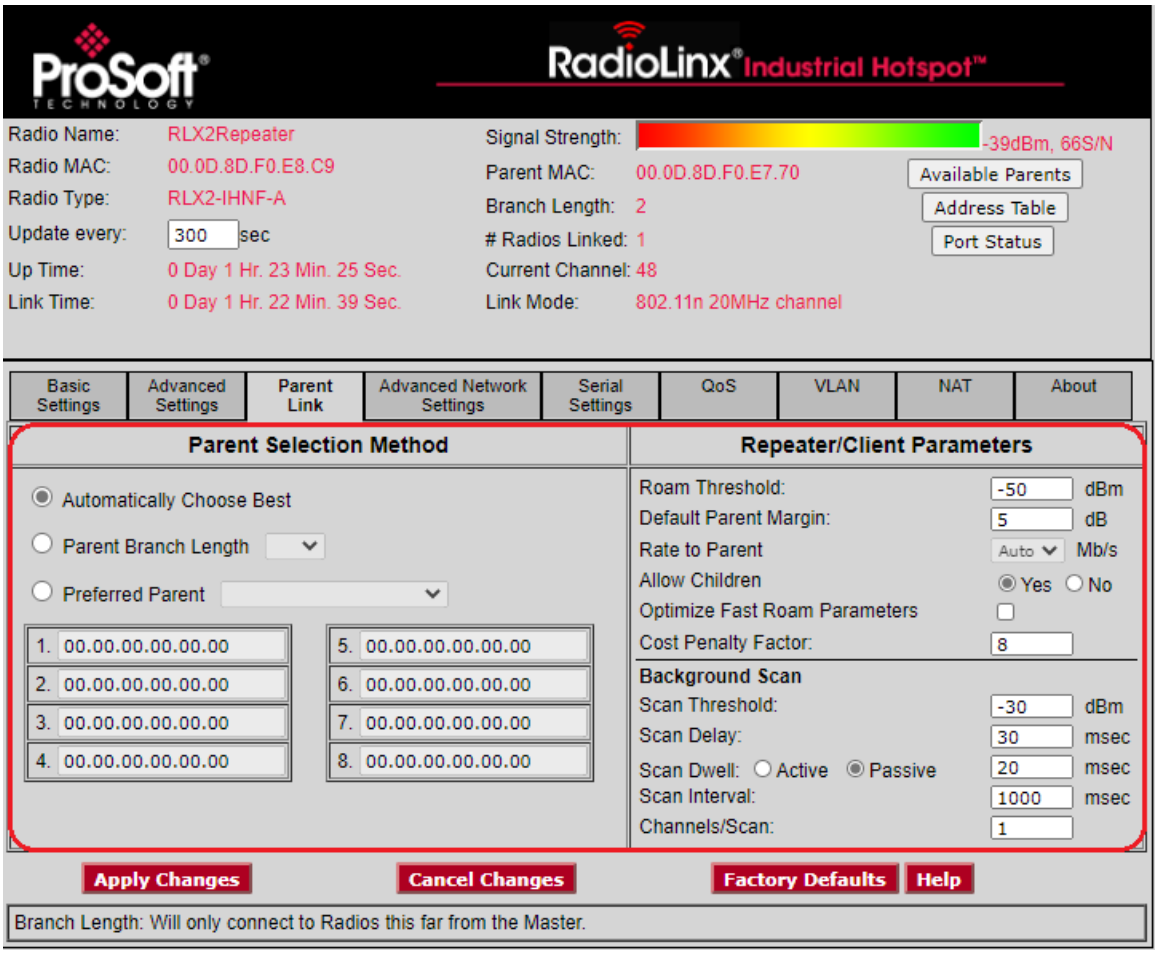
Note: Changing tabs and editing fields does not refresh this timer as those changes are local to the web browser. The ELXM-SW6 only restarts the login session timer if a webpage is refreshed, or the top info pane updates its information, or an **APPLY CHANGES** is done.

The *Update every* field defaults to the same value as the Timeout control. To keep the login session active, change the *Update* value to something smaller. For more information, see section *3.2 Viewing ELXM-SW6 Status*.

3.7 Configuring Parent Link Settings

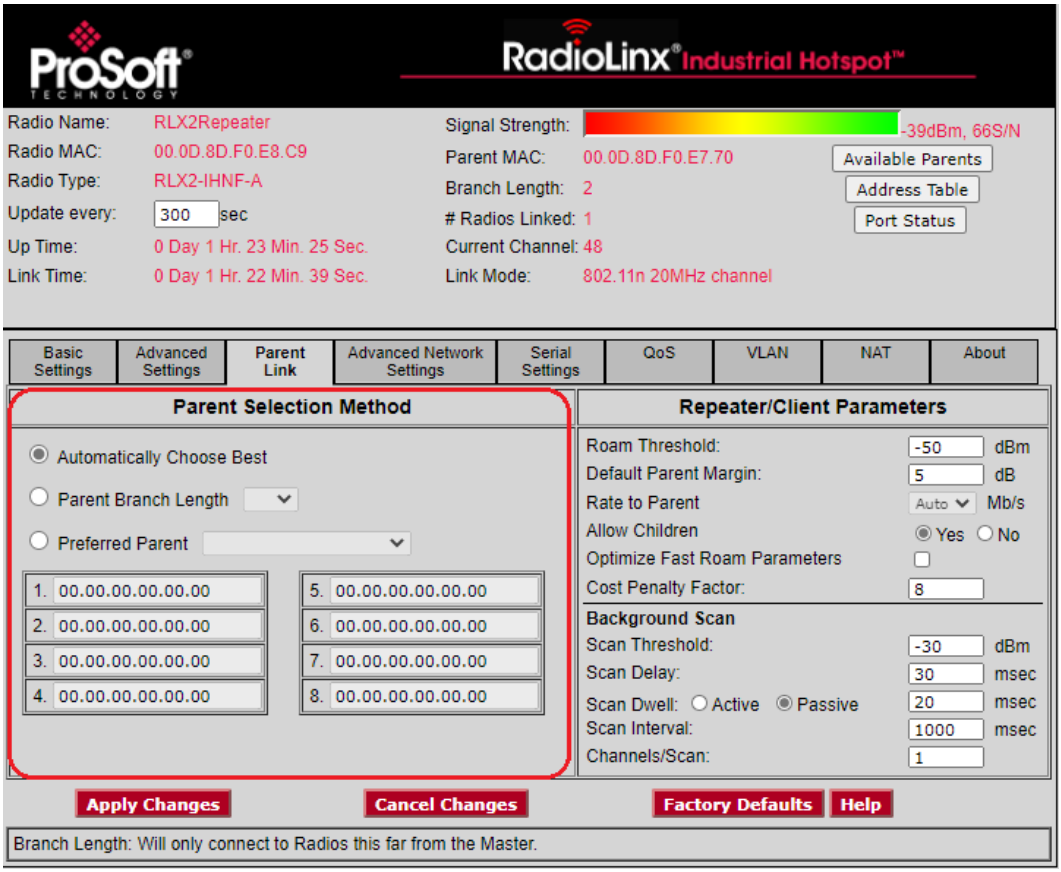
Use the *Parent Link* tab to specify how a ELXM-SW6 Client radio selects a Parent in order to connect to the network. The Parent Link includes two groups:

- Parent Selection Method
- Client Parameters



3.7.1 Parent Selection Method Settings

Use the parameters in the *Parent Selection Method* group to specify how the ELXM-SW6 Client radio chooses a Parent radio in a wireless network.

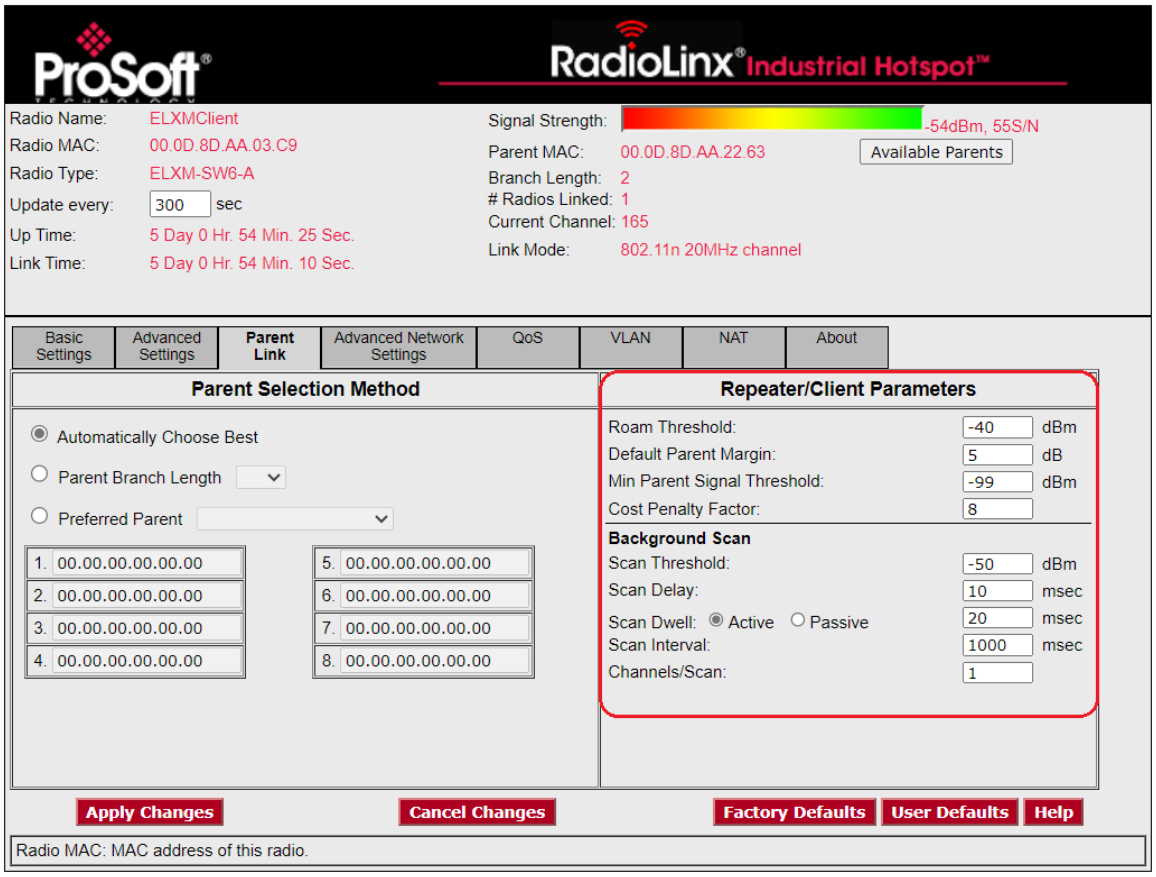


Parameter	Description
Automatically Choose Best	Calculates a "cost" metric for each possible parent radio that it detects and selects the Parent radio based on the lowest cost. The ELXM-SW6's calculation includes: • **RSSI**: Stronger signals receive a lower cost. • **Hop Count**: Fewer hops from the AP radio is given preference and lower cost
Parent Branch Length	Calculates the branch length to other radios and chooses the Parent radio strictly by the number of RLX2 Repeater radios between the ELXM-SW6 and the AP radio. If branch length of **1** is selected, the radio links only to the AP radio. If branch length of **2** is selected, the radio links only to a ProSoft Technology Radio with Repeater capability that is linked to the AP radio, and so on. If multiple candidate radios are available at a particular hop count, the ELXM-SW6 chooses the Parent radio that has the smallest cost as calculated by the Automatically Choose Best algorithm. **Note:** Branch Length is only a concept when using ProSoft Technology radios that support Repeater mode and can form multi-hop chains anchored at the AP. When the ELXM-SW6 is in Bridging Client mode and connecting to 3rd Party APs the Branch Length field is assumed to be 1.

Parameter	Description
Preferred Parent	Specifies how the ELXM-SW6 selects a Parent radio from the list of possible Parent radios. Specify a list of up to eight radios by entering the MAC addresses for each radio. The ELXM-SW6 chooses its Parent radio based on your selection for *Preferred Parent*: **BEST IN LIST:** The ELXM-SW6 selects its Parent radio using the Automatically Choose Best algorithm but limits the selection to the Preferred Parent list of radios. This selects the Parent radio in the list with the lowest cost. **FOLLOW LIST PRIORITY:** The ELXM-SW6 selects its Parent radio from the list giving preference to the 1st entry followed by the 2nd entry and so on. **2.4 GHZ PARENTS ONLY:** The ELXM-SW6 only selects a Parent radio from the list that is operating in the 2.4 GHz band. **5 GHZ PARENTS ONLY:** The ELXM-SW6 only selects a Parent radio from the list that is operating in the 5 GHz band.

3.7.2 Client Parameters Settings

Use the parameters in the **CLIENT PARAMETERS** group to specify the wireless communication parameters of an ELXM-SW6 Client radio.



Parameter	Description
Roam Threshold	Specifies a signal strength below which the ELXM-SW6 will roam to a Parent candidate with a stronger signal. For signals above that threshold, the ELXM-SW6 only gives preference to Parent radios with fewer hops from the AP radio.
Default Parent Margin	Specifies a minimum signal strength that any Parent candidate's signal strength must exceed the signal strength of the current Parent. Use this in Fast Roam applications where the ELXM-SW6 is on a mobile platform, or there is a lot of movement in the environment causing RSSI levels to fluctuate. The ELXM-SW6 keeps its current Parent unless another Parent's RSSI is stronger by this value. The ELXM-SW6 adds this margin value to the current Parent radio's RSSI prior to calculating its cost. The default value is 5 dB. • If the value entered is too small, it can lead to the ELXM-SW6 rapidly switching back and forth between two Parent radios as the RSSI levels change. • If the value entered is too large, it can result in preventing a Roam until the ELXM-SW6 moves out of range, even though a candidate exists that is better than the current Parent radio.

Min Parent Signal Threshold	Specifies the minimum signal strength a Parent Candidate must have before it can be picked as a new Parent. This control defaults to -99 dBm which effectively disables it. This control is useful on power up to ensure that an initial Scan for a Parent does not pick a Parent that is at extreme range, when it is known that a close-in Parent exists.
Cost Penalty Factor	Specifies the amount of penalty that is added to the current parent link due to Tx Failures. • A value of **0** uses the internal default of 8. • A value of **1** will disable the feature. • The maximum value accepted is **64**. The larger the factor, the higher the penalty. If the addition of the penalty forces a roam to an alternate parent, then the old parent will be excluded from any roam decisions until the penalty expires. For example, doubling this value will result in the ELXM-SW6 staying with the alternate parent twice as long before roaming back to the original parent, assuming the original parent still has the lowest cost.

3.7.2.1 Background Scan

The *Background Scan* group is used to modify the algorithm used by an ELXM-SW6 in a Client mode to search for parent candidates that may be on other channels.

The list of channels to be scanned for potential Parents is obtained from the current Parent, either from its Beacon or an explicit Neighbor Report request.

It is critical when doing a background scan that data loss be minimized or eliminated when switching to scan a radio channel different than that of the current Parent. When configuring these settings it is important to be cognizant of overall time the background scan will take, as that will add latency to data before it can be delivered after the background scan.

Latency = Scan Delay + (Scan Dwell x Channels-per-Scan)

The following steps are taken during a background scan attempt.

1. Signal the current parent that we are about to do a background scan.
2. Wait for ***Scan Delay*** time to receive any data packets sent by the parent before it was able to process our background scan signal.
3. Switch to another channel and Probe for an alternate parent that is using our SSID.
4. Wait for ***Scan Dwell*** time on this channel to receive any Probe Responses.
5. If the number of channels scanned is less than the *Channels/Scan* value go to Step 3.
6. Otherwise once ***Channels/Scan*** channels have been scanned, switch back to the current Parent's channel.
7. Signal the current parent that we have completed our background scan allowing it to send any data frames it has buffered since our signal in Step 1.

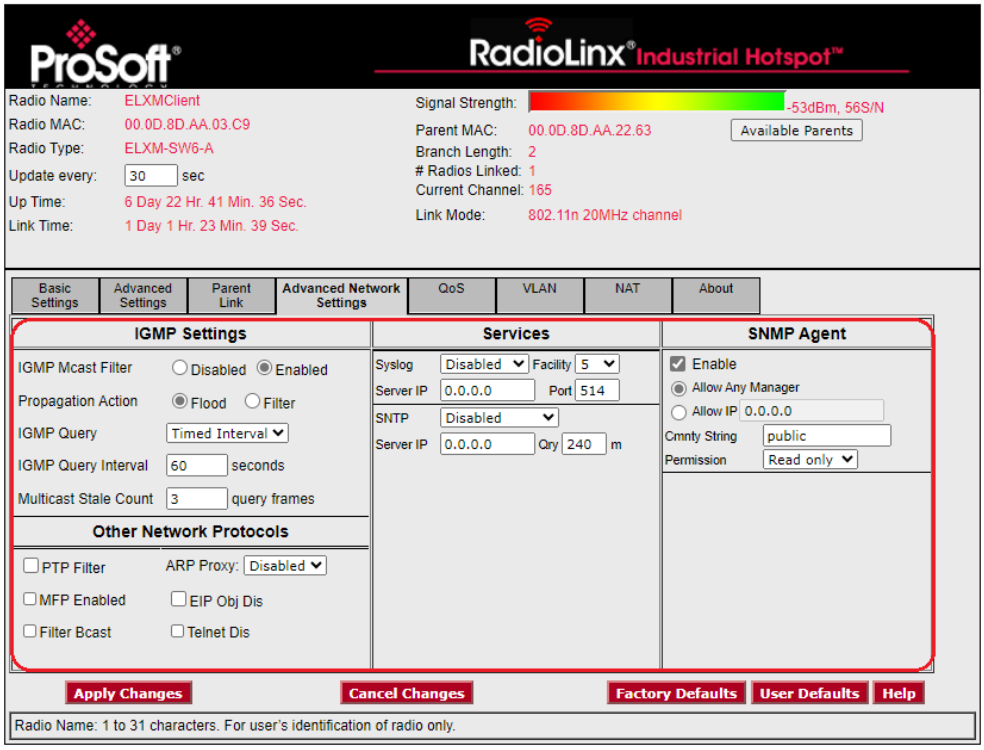
Parameter	Description
Scan Threshold	Background scans will be triggered if the current Parent's RSSI is below this threshold, with units of dBm. At each *Scan Interval* the ELXM-SW6 will scan the number of channels set by the *Channels/Scan* parameter before returning to the current Parent's channel and resuming normal operation. A value of **0** disables background scanning. Valid threshold values range from -30 to -99 dBm. Typically, this value should be set 5 to 10 dB lower than the *Roam Threshold* parameter so that when moving away for the current Parent, the best alternate Parent can be found prior to having to make a roam decision.
Scan Delay	This parameter is used when the ELXM-SW6 is in a Client mode and determines the amount of time the ELXM-SW6 will wait after having sent the AP a signal telling the AP that the ELXM-SW6 will be going off channel. This delay allows some time for the AP to deliver any data frames that have already been committed to the ELXM-SW6 hardware for transmission. Valid values range from **10** to **250** msec and must be a multiple of 10. This value should be as small as possible to minimize overall latency introduced by each background scan attempt, but large enough so that data is not lost each time a background scan is performed.
Scan Dwell	This parameter determines the amount of time in milliseconds that the ELXM-SW6 will wait on a channel to hear Beacons or responses to its Probe Request. The value must be a multiple of 10. The Radio buttons to the left of the *Scan Dwell* edit box configure whether the *Background Scan* will be Passive or Active. In a passive scan the ELXM-SW6 does not transmit a Probe Request but waits on the channel for the Dwell interval and processes any received Beacon. For this reason, a larger value for *Scan Dwell* should be configured when Passive is enabled, if possible, to increase chances of detecting a Beacon which are transmitted by APs typically every 100 msec. Passive Background Scans would be preferred when operating in a network where there are a very large number (>50) of ELXM-SW6 Client within range of each other on the same channel. Active Scanning under these conditions would use up a significant amount of a channel's bandwidth with Probe Requests and Probe Responses. In an active scan a Probe Request is sent to the channel to elicit a Probe Response from a potential parent candidate. The Probe Request contains the desired SSID, therefore only APs that are configured with that SSID will respond. **Note:** Given that Probe Requests are broadcast and may not be heard due to collisions with other traffic on the air, it may take multiple scans of a channel before a response is heard. The default value of 30 msec should be sufficient to receive any Probe Responses from a typical AP.

Scan Interval	The ELXM-SW6 will initiate background scans at every *Scan Interval* if the current Parent's RSSI is less than the value of the *Scan Threshold* parameter. Smaller values imply that background scans will occur more frequently whereas a larger value (up to 5 sec) imply it may take longer to find a Parent candidate on another channel. The value is in units of milliseconds and must be a multiple of 10.
Channels/Scan	This parameter determines the number of channels from the channel scan list that are scanned at each background scan interval. Each background scan starts from the channel after the last channel scanned on the last interval. **Note:** Normal data traffic is paused during a background scan, therefore the higher this number the longer the pause in data traffic flow.

3.8 Configuring Advanced Network Settings

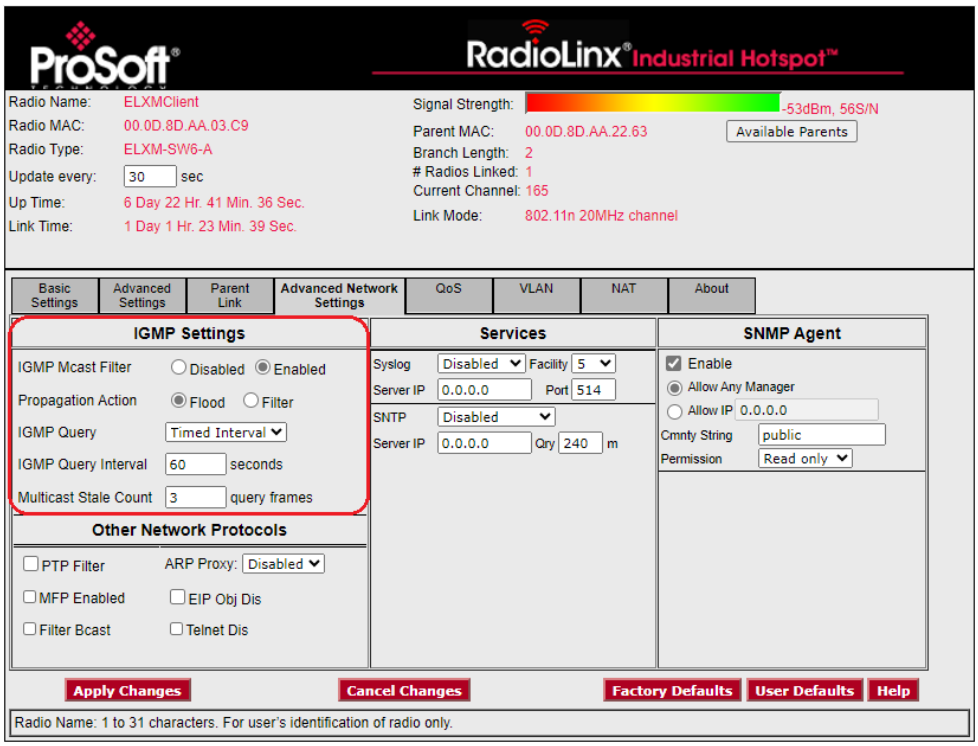
Use the *Advanced Network Settings* tab to specify the IGMP (Internet Group Management Protocol), STP (Spanning Tree Protocol), SNMP (Simple Network Management Protocol), and Location Services parameters for the ELXM-SW6. The *Advanced Network Settings* includes the following groups:

- IGMP Settings
- Services
- SNMP Agent
- Other Network Protocols



3.8.1 IGMP Settings

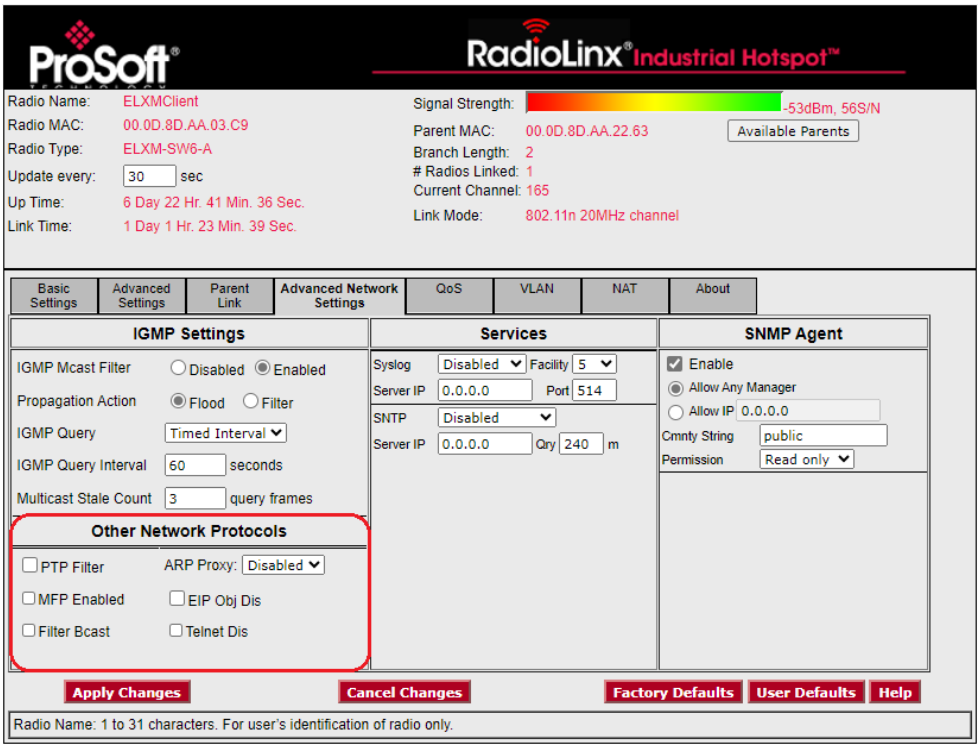
Use the parameters in the *IGMP Setting* group to specify the Internet Group Management Protocol parameters of the ELXM-SW6. The ELXM-SW6 supports IGMP v1 and v2. The IGMP functions are enabled by default.



Parameter	Description
IGMP Multicast Filtering	Specifies the state of IGMP multicast filtering (**DISABLED** or **ENABLED**).
Default Propagation Action	Specifies how the ELXM-SW6 handles multicast addresses that are not in the ELXM-SW6's address table. **FLOOD:** The ELXM-SW6 sends unknown multicast packets to all ports. **FILTER:** The ELXM-SW6 filters unknown multicast packets and does not send them to any ports.
IGMP Query Generation	Specifies the state of IGMP query generation in the ELXM-SW6. **DISABLED:** Disables IGMP query generation. **TIMED INTERVAL:** Enables IGMP query generation. Use IGMP Query Interval to specify the query time interval.
IGMP Query Interval	Specifies the number of seconds between queries (if the timer is not pre-empted by a query from another device). By RFC specification, only one device on a network should generate IGMP queries. As such, the ELXM-SW6 only sends an IGMP query if another device has not sent a query within the ELXM-SW6's *IGMP Query Interval* setting, even if *IGMP Query Generation* is enabled.
Multicast State Count	Specifies the number of queries the ELXM-SW6 generates before a device is removed from the multicast group on the ELXM-SW6 if no response is received from the device.

3.8.2 Other Network Protocols

This section contains controls to enable or disable actions taken on PTP or ARP packets received on the ELXM-SW6 Ethernet interface.

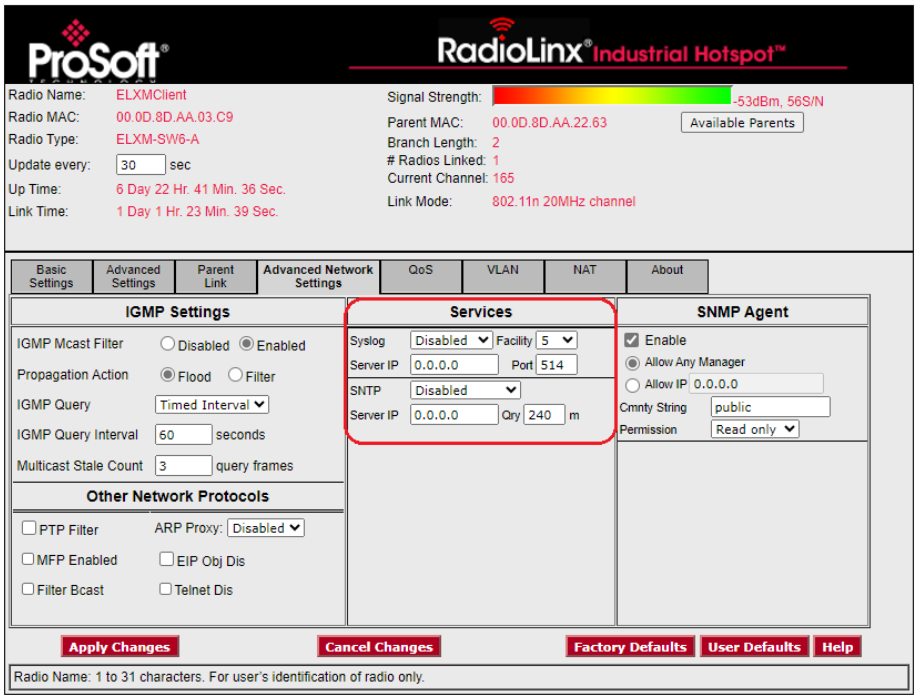


Parameter	Description
PTP Filter	Check this box to enable the PTP Filter feature. The Precision Time Protocol (PTP) is used in industrial networks to synchronize time between devices. Given the protocol uses multicast addressing, a PTP packet sent by one device is sent over every wireless link in that network. PTP is only needed amongst a set of locally Ethernet connected ELXM-SW6's. The injection of PTP packets arriving over a wireless link (connecting this local network to the main network) may cause large errors in time synchronization. To prevent leaking of PTP packets, the following control allows the ELXM-SW6 to filter any PTP packets received on its Ethernet port. When this capability is desired, this control should be enabled on all APs and Clients in the network
MFP Enabled	Check this box to enable 802.11w Management Frame Protection in the ELXM-SW6. MFP when enabled, requires that management frames received over a wireless connection must be encrypted. Management frames received from a Parent or child node that are not encrypted are discarded, preventing denial of service attacks. When MFP is enabled the ELXM-SW6 will always encrypt management frames that it sends to an Associated peer/client. Both ends of a wireless link must have MFP enabled before MFP will be used on that link. If the peer/client does not have MFP active (as indicated in Beacons and Associate Request elements) then the ELXM-SW6 will not use MFP on that link, even if this control is checked. **Note:** This control is automatically disabled if the Security Mode configured on the Basic Settings tab does not include WPA2.

Parameter	Description
ARP Proxy	In industrial wireless networks, it is important to minimize external disturbances which can cause packet latencies to soar. This can be anything from interference generated from other equipment to another wireless network using the same channel or even internally generated broadcast bursts which when transmitted simultaneously from multiple overlapping APs can cause severe latency spikes. The latter can sometimes unintentionally be caused by a controller looking for a list of remote devices, producing a burst of ARP Request frames. The ARP Proxy feature when enabled, will intercept these ARP Requests, and prevent them from flooding the wireless network. The ELXM-SW6 is continually learning and adding the MAC and IP Addresses of devices to its address tables and if the IP Address being requested by the ARP Request is known, the ARP Proxy function will send an ARP Response for the IP Address back to the Requestor and not forward the ARP Request to the wireless interface. The ARP Proxy modes that are supported are: **DISABLED:** Disables the ARP Proxy feature. Any ARP Request received on the Ethernet will be forwarded to the ELXM-SW6 interface. **FILTER:** ARP Requests that are received on the Ethernet interface are always filtered and not forwarded to the ELXM-SW6 interface. If the Target Address in the ARP body is known to belong to a peer radio, then an ARP Response will be directed back to the requestor. **ALLOW:** ARP Requests received on the Ethernet interface with a Target Address is known to belong to a peer radio are filtered and an ARP Response is directed back to the requestor. All other ARP Requests are forwarded to the ELXM-SW6 interface. The ARP Proxy feature should be “Disabled” or set to “Allow” if it is known that remote devices do not send unsolicited IP frames after power up. If the device remains silent until it is polled for example, then the ELXM-SW6s will not learn its IP/MAC Address and any ARP Requests for this device will not reach it if the ARP Proxy feature is set to “Filter”. In wireless network topologies where Clients always connect directly to APs, the ARP Proxy feature only needs to be enabled on the APs.
EIP Object Disable	Check this box to disable the Ethernet I/P agent in the ELXM-SW6. When checked queries to read the EIP Object classes are ignored. It should be noted that the EIP module is read-only and the "Get" responses include certain settings as well as status of the ELXM-SW6, but they do not include any security related 'secret' data. This control is provided for those customers that wish to shut down any interface that is not required for their application.
Filter Bcast	Check this box to disable propagating broadcast and multicast packets from the Ethernet interface to the Wireless interface. All broadcast/multicast packets are filtered except for ARP, DHCP and IGMP type packets. ARP and IGMP filtering is handled by the ARP Proxy and IGMP functions of the ELXM-SW6. Broadcasts and multicasts received from the Wireless interface are not affected.
Telnet Dis	Check this box to disable the Telnet interface on the ELXM-SW6. On the ELXM-SW6 the telnet interface connects to an internal log where diagnostic and status prints are output. This does not access a login shell in the operating system, and no security related data can be viewed from this interface. This control is provided for those customers that wish to shut down any interface that is not required for their application.

3.8.3 Services

Use the parameters in the Services group to configure features that aid in diagnosis of the ELXM-SW6's activities.



3.8.3.1 Syslog

Use the parameters in the *Syslog* group to configure the ELXM-SW6 Syslog service. Syslog UDP messages containing information about the current state and events during operation of the ELXM-SW6 are sent to an external Syslog Server that records the messages. These messages are time-stamped and can be reviewed to perform diagnosis and analysis of any system or wireless issues that may have occurred.

Parameter	Description
Syslog	**DISABLED:** The Syslog feature is disabled, and no Syslog messages will be sent from the ELXM-SW6. **ENABLED:** The Syslog feature is enabled, and Syslog messages will be sent to the Server IP and Port number specified.
Facility	This sets the Facility number that will be encoded into each Syslog message sent by the ELXM-SW6. The User Facility levels Local 0 through Local 7 can be selected as specified by the network Administrator where the ELXM-SW6 is installed.
Server IP	This specifies the external Syslog Server IP Address to which all syslog messages will be sent.
Port	This specifies the UDP Port number that the external Syslog Server is listening.

3.8.3.2 SNTP

Use the parameters in the *SNTP* group to configure the ELXM-SW6 Simple Network Time Protocol (SNTP) service. Using SNTP, the ELXM-SW6 can accurately set its system time so that timestamps in Syslog messages reflect 'real' time.

The ELXM-SW6 uses a SuperCAP to maintain its on-board real-time clock for up to 48 hours when power is removed. If power is removed for an extended time, on startup, the ELXM-SW6 initializes its system time to a built-in value representing when the firmware image was compiled. Since each ELXM-SW6 may start up at a different instant, their system times relative to each other are uncorrelated.

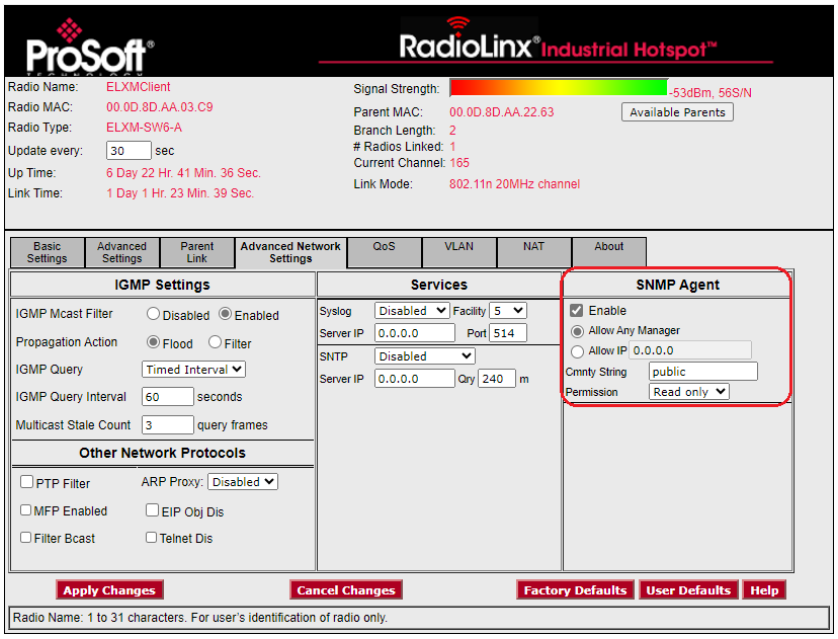
Note that a time jump may occur in syslog messages a few seconds after startup, when the system time is updated after receiving an SNTP response from the SNTP Server.

Parameter	Description
SNTP	**DISABLED:** The SNTP feature is disabled and no SNTP messages will be sent from the ELXM-SW6. **ENABLED:** The SNTP feature is enabled and SNTP messages will be periodically sent to the Server IP to keep the ELXM-SW6's internal system time synchronized to the SNTP Server's 'real' time.
Server IP	This control specifies the external SNTP Server IP Address to which all SNTP Query messages will be sent. The SNTP protocol uses the standard port number of 123.
Qry	This control specified the interval that the ELXM-SW6 sends SNTP Queries to the SNTP Server. The interval is in units of minutes. Since the internal system clock of the ELXM-SW6 is quite accurate, frequent queries to the SNTP Server are not necessary. The default value for this parameter is 240 minutes

3.8.4 SNMP Agent

Use the parameters in the **SNMP AGENT** group to specify the Simple Network Management Protocol parameters of the ELXM-SW6.

SNMP is a network management protocol that is often used with TCP/IP and Ethernet. It offers an alternative to using the ELXM-SW6 web interface, and allows you to use an SNMP manager application to change ELXM-SW6 settings and view diagnostics.

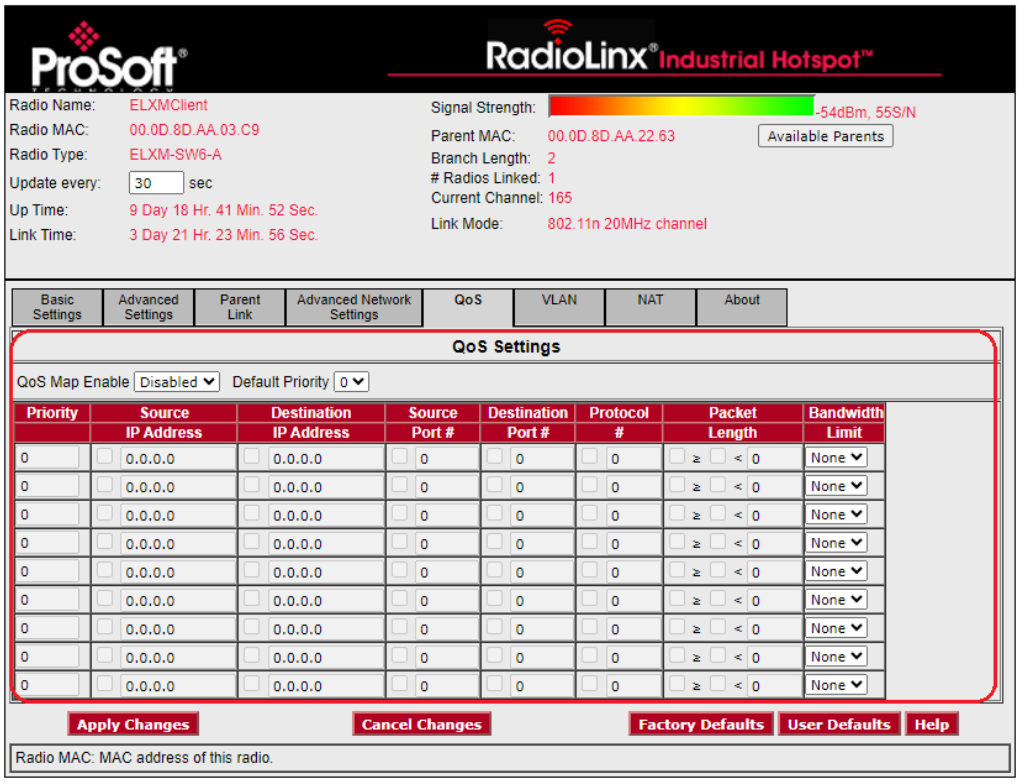


Parameter	Description
Enable	Select this check box to enable the following SNMP agent.
Allow Any Manager	Specifies that any user can change the ELXM-SW6 configuration from any computer using SNMP.
Allow IP	Specifies that only an SNMP manager with a particular IP address can change the ELXM-SW6 configuration. You must enter the IP address.
Community String	Specifies a community string (like a password) that an SNTP manager must use to access the ELXM-SW6's SNMP agent.
Permission	Specifies the permission level to assign to the ELXM-SW6. **READ ONLY:** The SNMP manager can only view the ELXM-SW6 configuration. **READ/WRITE:** The SNMP manager can view and edit the ELXM-SW6 configuration.

- The ELXM-SW6's SNMP agent supports SNMP protocol version 1.4 and 2.
- MIBs:
  - RFC12133-MIB (partial; internet.mgmt.MIB-2.system, .interfaces, .snmp)
  - ROMAP-MIB (internet.private.enterprises.romap)
- It also supports a selection of standard SNMP traps, including Cold Start, which the ELXM-SW6 sends when it initializes.

3.9 Configuring Quality of Service (QoS) Settings

Use the *QOS Settings* tab to specify the packet priority value parameters for the ELXM-SW6.



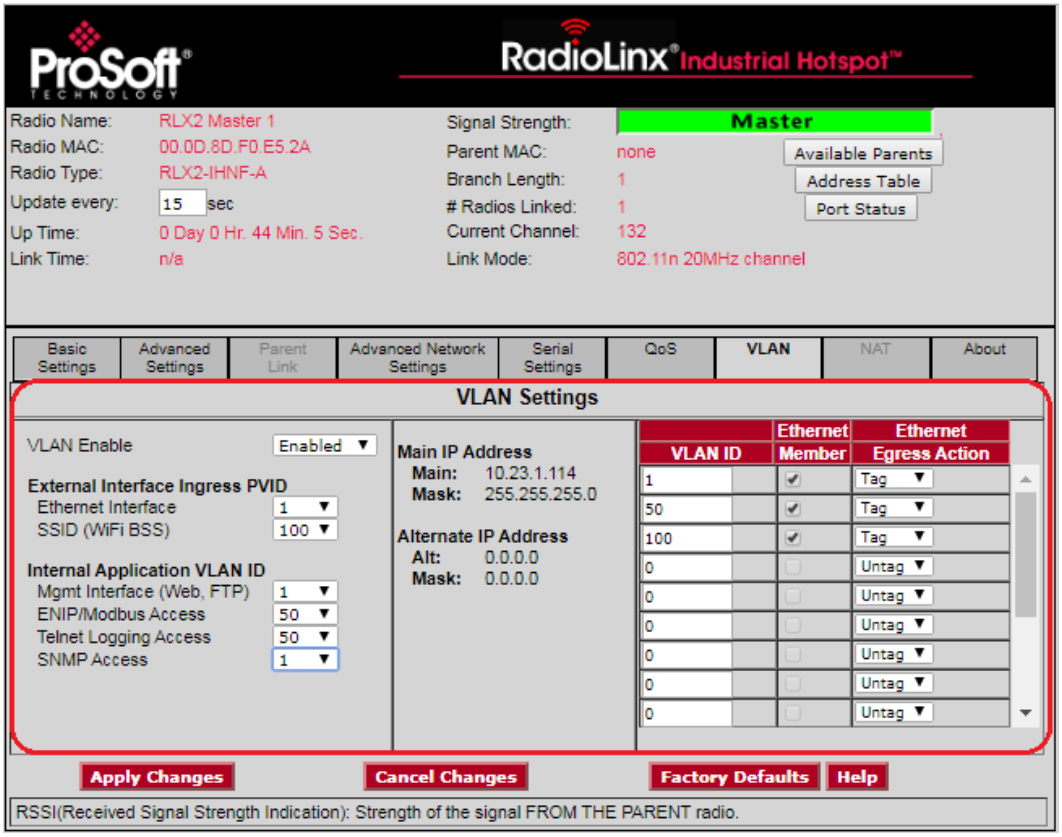
The ELXM-SW6 prioritizes frames using QoS for packets received already marked with a priority value. The *QOS Settings* tab allows you to set the default priority for frames that the ELXM-SW6 receives without any priority markings. In addition, priority values can be mapped to packets received without priority markings according to a set of matching criteria.

Parameter	Description
QoS Map Enable	Specifies whether the ELXM-SW6 uses the priority mapping function. **ENABLED -** The ELXM-SW6 uses the Default Priority and the priority mapping table to prioritize packets received on the ELXM-SW6 Ethernet interface, without a priority value. You must select Enabled before you can edit the QoS Map table. **DISABLED -** The ELXM-SW6 does not set priority values for Ethernet packets received without a priority value.
Default Priority	Specifies the default priority for packets received on the Ethernet interface without a priority value (default is 0: no priority).

Parameter	Description
QoS Map Table	Specifies up to nine separate match criteria to identify and assign priority values to received Ethernet packets. Each filter has several parameters that you can enable by selecting the check box to the left of each parameter. When you enable multiple parameters in a row, all enabled parameters in that row must match before the ELXM-SW6 assigns the specified *Priority* value to a packet. **PRIORITY:** The priority value the ELXM-SW6 assigns to the received Ethernet frame if it was not already marked with a priority value and if all enabled parameters in the same row match. **SOURCE IP ADDRESS:** A parameter match occurs for all packets received from the device with this source IP address. **DESTINATION IP ADDRESS:** A parameter match occurs for all packets received addressed to the device with this destination IP address. **SOURCE PORT NO.:** A parameter match occurs for all IP packets received with this source port value. **DEST PORT NO.:** A parameter match occurs for all IP packets received with this destination port value. **PROTOCOL NO.:** A parameter match occurs for all IP packets received with this protocol number. **PACKET LENGTH:** A parameter match occurs for all iP packets received with the correct packet length. • Enter a packet length threshold. • Select the match criteria. • Select < to match if the length of the received packet is **LESS THAN** the threshold. • Select ≥ to match if the length is **GREATER THAN OR EQUAL TO** the threshold. • Select both < and ≥ to match **ALL PACKET LENGTHS**.
Bandwidth Limit	Specifies whether packets that match the rule will have bandwidth limitations imposed on them. **Note:** This control is only available when the Protocol Number filter is set to TCP (6). When set to **NONE** no bandwidth limitation will be applied. This means that a TCP Stream that matches the filter can potentially use all the channel bandwidth. Setting this control to **HIGH, MEDIUM** or **LOW** will respectively reduce the percentage of the max bandwidth that a matching TCP stream will utilize effectively reserving the remaining bandwidth for other traffic of the same or lower priority. **Setting** / **Limit w / 1 stream** / **Limit w / 2 streams** High / 80% / 60% Medium / 60% / 40% Low / 50% / 30%

3.10 Configuring VLAN Settings

Use the **VLAN** tab to specify the Virtual Local Area Network parameters of the ELXM-SW6. When the ELXM-SW6 sends a packet, it includes the configured VLAN ID.



ELXM-SW6's support port based VLANs. Each ELXM-SW6 can be considered to have 3 different ports or interfaces; the Ethernet interface, the local applications stack of the ELXM-SW6 itself, and the 802.11 BSS created by each AP.

Configure the VLAN settings for the Ethernet interface on all ELXM-SW6's. You can only configure the VLAN for the Internal Application and SSID ports on a ProSoft Technology AP radio. The ProSoft Technology AP radio pushes these settings to each connected ELXM-SW6 Client radio. This allows the VLAN settings for a bridged network rooted at an AP radio to have common settings for these ports. For example, this ensures that if the Local interface is set to a management VLAN, then all Client radios are accessible from a Management PC.

To facilitate customer networks that use VLANs to separate management of network components from operational functions, the ELXM-SW6 can assign different VLAN IDs to these functions. This allows the configuration and firmware upgrade functions to be accessible only from a management VLAN, leaving the ENIP module on an operational VLAN so it can be accessed by PLCs or Master Controllers.

In the example configuration above, the ProSoft AP is configured with three VLANs forming a trunk link on the AP's Ethernet interface. The management VLAN has VLAN ID of **1**, the operational VLAN has VLAN ID of **50** and a user wireless access network has a VLAN ID of **100**.

This configuration assumes the AP is connected to a managed switch that is VLAN capable. Settings changes can only be done from VLAN 1 (the management VLAN). Users connecting directly to the AP wirelessly can neither make settings changes nor can they access the operational network.

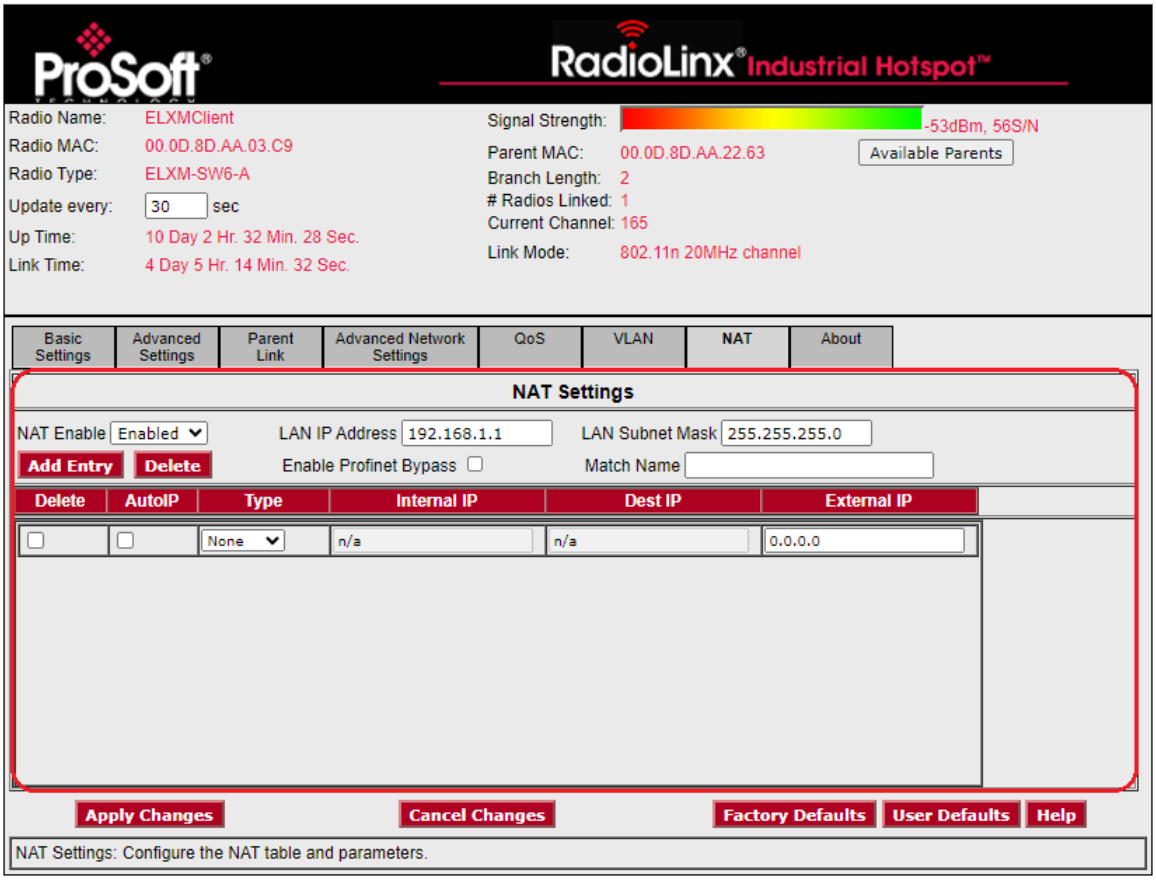
For customer networks that assign a different subnet on each VLAN, the ELXM-SW6 supports the configuration of a 2nd Alternate IP Address via the *Basic Settings* > *Access Setting* section of the ELXM-SW6 webpage. This allows the internal applications to be accessed with either IP Address if the packet is tagged with the VLAN ID assigned to that application.

For more information, see Chapter *6 Appendix B - ELXM-SW6 Virtual LAN (VLAN) Functionality*.

Parameter	Description
VLAN Enable	Select this check box to enable the VLAN function of the ELXM-SW6. • When enabled, packets received by the ELXM-SW6 on an interface that are not VLAN tagged are assigned to the VLAN as set by the PVID parameter of the respective interface. • When disabled, the ELXM-SW6 still bridges received Ethernet packets that are VLAN tagged but does not act on the VLAN ID of the frame or add or remove any VLAN tags.
Ethernet (ingress) PVID SSID (ingress) PVID	Specifies the PVID setting; representing the VLAN ID to assign to non-tagged ingress frames from each interface (Ethernet, SSID).
Internal Application VLAN ID	Specifies the VLAN ID to assign to applications on the ELXM-SW6. • The *Mgmt Interface* setting assigns a VLAN ID to the Web and FTP servers, allowing configuration and firmware update access. • The *ENIP/Modbus* setting assigns a VLAN ID to the ENIP and Modbus agents, allowing access to those modules from PLCs only from the assigned VLAN. • The *Telnet* setting assigns a VLAN ID to the Telnet Server, allowing logging access by a Telnet Client (Ex. IH Browser) only from the assigned VLAN. • The *SNMP* setting assigns a VLAN ID to the SNMP Agent, allowing access by SNMP Managers from the assigned VLAN.
VLAN Settings	Specifies the details for each VLAN. Use the VLAN Table to add a VLAN ID to the ELXM-SW6 and specify whether the Ethernet interface is a member of that VLAN and whether egress frames should be tagged or untagged for a particular VLAN. Configure up to 15 different VLAN ID's. **VLAN ID:** The ID of the VLAN to be included on this ELXM-SW6. Valid VLAN ID's range from **1** to **4096**. Note that VLAN ID's 1956 and 1957 are reserved and cannot be used. **ETHERNET MEMBER:** Specifies whether to make the Ethernet interface of the ELXM-SW6 a member of the VLAN indicated by the row's VLAN ID. **ETHERNET EGRESS ACTION:** Specifies whether frames belonging to the row's VLAN ID are sent out the Ethernet port as **TAGGED** or **UNTAGGED**.

3.11 Configuring NAT Settings

Use the NAT tab to specify the Network Address Translation parameters of the ELXM-SW6. This feature maps a set of external IP Addresses to internal 'private' IP Addresses in a 1:1 manner.



When NAT is enabled, the ELXM-SW6 Ethernet port becomes the default gateway for the internal private network and the wireless interface provides access to the external network. The IP Address configured for the ELXM-SW6 via the *Basic Settings* Tab must be valid on the external network. The IP Address used by the ELXM-SW6 for the internal network must be configured as the default gateway on all devices on that internal network and is configured via the *NAT* tab in the *LAN IP Address* and *LAN Subnet Mask* fields.

There are 2 types of NAT entries: *1:1 Src* entries and *1:1 Dst* entries. All devices on the internal network that wish to access or wish to be accessed from the external network must have a 1:1 Src entry in the NAT table to translate their internal IP Address to an external IP Address. This means that the most devices that an ELXM-SW6 can support on the internal network is 16 (max NAT Table size), when NAT is enabled.

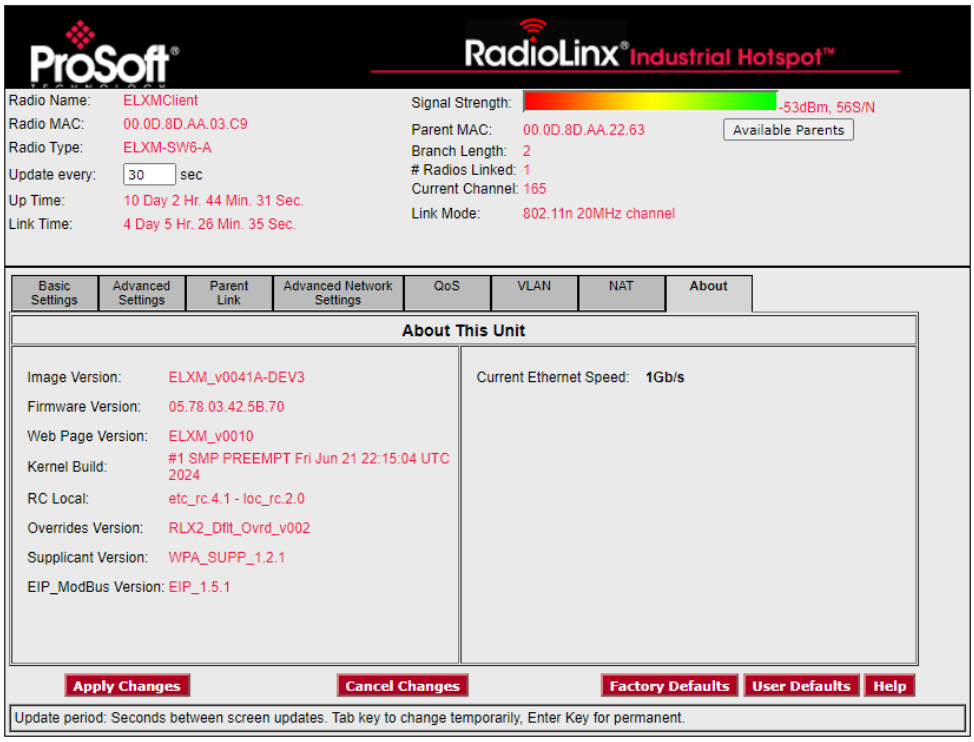
The 1:1 Dst type entries allow a device on the internal network to address a device on the external network using a local internal IP Address. This entry type is not often used, but does allow configuration of devices on the internal network to be agnostic of any external IP Address, relying on the NAT table to map a 'standard' set of local external IP Addresses to their actual external equivalents.

Parameter	Description
NAT Enable	Specifies to enable or disable the NAT function of the ELXM-SW6. NAT is only available if the ELXM-SW6 is in Ethernet Bridge or Bridging Client modes. In AP or Client modes the NAT Tab is disabled. If NAT is disabled, then no Network Address Translation (NAT) occurs and the ELXM-SW6 operates in normal Ethernet Bridge or Bridging Client mode. If NAT is enabled, the source IP Address and optionally the destination IP Address of packets going from the ELXM-SW6 Ethernet to the wireless interface are translated according to the NAT Table entries for those IP Addresses. The reverse translations occur for packets going from the wireless interface to the ELXM-SW6 Ethernet.
LAN IP Address	Specifies the IP Address the ELXM-SW6 uses for its Ethernet interface. When NAT is enabled the ELXM-SW6 operates like a NAT router and this IP Address must also be the default gateway for the internal private network. The default for this IP Address is **192.168.1.1** and should be changed if a different subnet is desired for the internal network.
LAN Subnet Mask	The LAN Subnet Mask defaults to **255.255.255.0** to match type C address default for the LAN IP Address. It is important to set the subnet mask correctly on the ELXM-SW6 and that it matches the subnet mask configured in each of the Ethernet devices on the internal network.
Enable PROFINET Bypass	Specifies a single device's PROFINET layer 2, non-IP packets, to bypass the NAT layer and transit the ELXM-SW6 from Ethernet-to-Radio or Radio-to-Ethernet. The first PROFINET device detected on the ELXM-SW6 Ethernet whose PROFINET Name contains the *Match Name* value, will have its PROFINET packets bypass the NAT layer. To enable a PROFINET connection to be configured, a NAT entry must also be added for the PROFINET device, to properly translate its TCP and UDP traffic between the local and remote subnets. **Note:** The PROFINET Bypass feature is only active if NAT is enabled.
Match Name	Specifies a common part of a local device's PROFINET Name that must match for its PROFINET packets to bypass the NAT layer. **Example:** In an automated guided vehicle application where the same configuration is required on each AGV, if the PROFINET Names of the PLCs on the AGVs are **'acme-agv-01**', '**acme-agv-02**' ... **'acme-agv-xx**', then the *Match Name* can be set to **'acme-agv-**' to match the local PLC Name on each AGV. Care must be taken when assigning PROFINET Names to local devices to ensure that the *Match Name* will only result in a match to the intended device and not to any other PROFINET device on the local network. The *Match Name* can be up to 31 characters and can only consist of valid PROFINET Name characters: **0-9**, **a-z**,., and **-**.
Add Entry	Specifies to add a new entry to the NAT table. Up to 16 entries can be present in the NAT table. The fields of the entry must be set according to the type of translation and the IP Addresses to be translated. Note that the entry is only saved once the **APPLY CHANGES** button is clicked.
Delete	This button is used to remove selected entries from the NAT table. When pressed any entries that have the checkbox in the Delete column checked, will be removed from the list. Once an Apply Changes is done the entry is permanently removed. If the webpage is refreshed prior to clicking **APPLY CHANGES**, then the original NAT entries will repopulate the list.

Parameter	Description
NAT Table	The NAT Table contains entries that inform the NAT function on the type of translation and on which IP Addresses the translation should occur. Each field of an entry row is described below: **DELETE:** Rows that have this checkbox checked will be removed from the NAT table if the Delete button is pressed. **AUTOIP:** When checked this indicates that the External IP Address field will be calculated based on the main IP Address of the ELXM-SW6 using the following formula: *Ext IP Addr* = ELXM-SW6 IP Address + offset, where offset = 1 and is incremented for each row encountered that has the AutoIP checkbox selected, down the table. The main benefit of this feature is to enable an IP Address assignment plan that only requires one IP Address setting on the ELXM-SW6, allowing the configuration to be cloned to multiple identical networks each with the same internal IP Addresses but differing only in the one external IP Address that is configured. **TYPE:** The type of 1:1 NAT translation to be done. Either 1:1 Src or 1:1 Dst must be selected. The appropriate IP Address fields in the entry will be enabled depending on the setting. **INTERNAL IP:** The IP Address of a device on the internal network that will be translated to the IP Address in the External IP field of this row of the table, for packets going from Ethernet to wireless. The reverse translation occurs on the destination IP Address of packets going from wireless to Ethernet that match an External IP Address in the NAT Table. If the entry is a 1:1 Src type then the destination IP Address in the packet is translated to the Src IP Address in the entry. **DEST IP:** The internal IP Address representing an external device. When this IP Address appears as the destination of a packet going from the Ethernet to wireless it will be translated to the External IP Address of the entry. The reverse translation occurs on the Source IP Address of packets going from wireless to Ethernet that match an External IP Address in the NAT Table. If the entry is a 1:1 Dst type then the source IP Address is translated to the Dest IP Address in the entry. **EXTERNAL IP:** An IP Address on the external network that is translated to/from internal IP Addresses that are in the NAT Table.

3.12 About This Unit

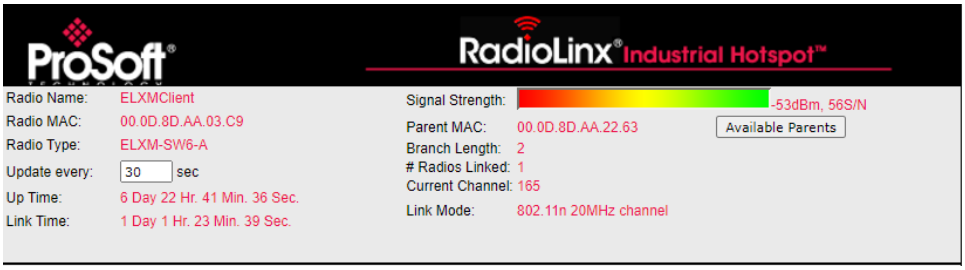
This tab displays the version of various modules that have been loaded and are running in the ELXM-SW6.



Parameter	Description
Image Version	Specifies the software version that was last loaded into the ELXM-SW6. Example: *ELXM_v0041A*. This Software Image is available for download from the ProSoft website. This Software Image is a combo image that contains many sub-components.
Firmware Version	Specifies the main radio driver version number and is one sub-component of a Software Image.
Webpage Version	Specifies the version of the webpages that are available for management of the ELXM-SW6 via its web interface.
Kernel Build	This date identifies when the OS kernel running in the ELXM-SW6 was built.
Overrides Version	Specifies the version of the default override file that is also a sub-component of the Software Image. The override file would only be different when custom default overrides have been included in a special Software Image.
Supplicant Version	Specifies the version of the WPA Supplicant that is responsible for Enterprise level Security.
EIP-Modbus Version	Specifies the version of the EtherNet/IP / Modbus Agent that allows observation of radio status and parameters using EtherNet/IP or Modbus queries.

4 Diagnostics and Troubleshooting

Use the IH Browser's diagnostic and signal strength settings at the top of the *Radio Settings* window to make sure the network is working properly:



- **Signal Strength**: Specifies the ELXM-SW6's signal strength.
  - *AP* appears if this is an AP radio.
  - *Scanning* appears if the ELXM-SW6 is scanning to connect to another radio.
  - *Not Connected* appears if the ELXM-SW6 is not connected to a network and not currently scanning.
- **Update every:** Specifies the interval (in seconds) between updates. The default value is 300 seconds which corresponds to the login timeout of the web interface. Entering a smaller value will allow the update to reset the session timer.
- The other parameters on this display are Read-only.

Tip: To display the help topic for any parameter, click on the parameter name.

Perform the following troubleshooting routines:

- Check the Ethernet cable
- Check the LEDs on the ELXM-SW6
- Retrieve the default password by resetting the ELXM-SW6 to factory or user defaults
- View error messages in the IH Browser
- Find missing radios

4.1 Checking the Ethernet Cable

If the ELXM-SW6's Ethernet port is connected to a PC or network, and the Ethernet LED does not light on the ELXM-SW6, there may be a problem with the Ethernet cable. Verify that the cable is plugged into the ELXM-SW6 at one end, and to a PC, or a 10/100/1000 Base-T Ethernet switch at the other end.

If using a PoE injector, verify that the RJ45 cable is connected between the radio and the injector and also that the Ethernet patch cable is connected between the injector and the switch.

Note: The ELXM-SW6 auto-detects the Ethernet connection type and does not require a crossover cable for a direct connection to a PC.

4.2 LED Display

The ELXM-SW6 front panel includes a set of LEDs that indicate the ELXM-SW6's status.

LED	LED	Description
POWER		Booting up
		Operational This two-color LED turns amber when power is first applied. It then turns green when initialization begins.
ACTIVITY		During ELXM-SW6 initialization.
		Blinking: Transmitting or Receiving data over the wireless interface.
SIGNAL STRENGTH		Loading OS – will turn on for ~ 1 sec and then turn off.
		Blinks if SD card inserted with new configuration. This is for all radio modes.
		ELXM-SW6's in AP mode:
		No radios linked
		One or more radios linked (right LED blinking).
		DFS Channel Availability Check in progress (all LEDs blinking Amber)
		ELXM-SW6's in Bridge or Client mode:
		No Signal
		Radio linked, Poor Signal
		Radio linked, Fair Signal
		Radio linked, Good Signal

The following LEDs illuminate when power is applied and the ELXM-SW6 is connected to the network.

- The POWER LED is green.
- The LINK LED on the Ethernet connector indicates a valid wired link. This LED is located at the bottom of the Ethernet RJ-45 connector and is marked LINK
  - OFF: 10 MB
  - ON: 100 MB
  - BLINK: 1 GB
- The ACTIVITY LED on the Ethernet connector blinks occasionally indicating Ethernet transmit and/or receive activity.
- The wireless ACTIVITY LED below the POWER LED starts to occasionally blink.

For ELXM-SW6's in Bridge or Client mode, all three SIGNAL STRENGTH LEDs blink just after the ELXM-SW6 links to the AP radio and before fully authenticating the link. Normally this lasts less than a second. If the SIGNAL STRENGTH LEDs blink for longer than a few seconds, or do not stop blinking, it usually means the encryption keys are not correct. The Wireless Security Settings on a Client radio must match those on the AP radio. For more information, see section *2.5 Configuring an ELXM-SW6 - Getting Started*.

4.3 Resetting the ELXM-SW6 to Defaults

If the password to the ELXM-SW6 is lost, the ELXM-SW6 settings cannot be changed. The ELXM-SW6 can be factory reset to restore the default password, but the ELXM-SW6 loses all configuration settings and returns to default settings.

4.3.1 Resetting to Factory Defaults

The following steps reset the ELXM-SW6 to its default settings, including the default password.

1. Remove power from the ELXM-SW6.
2. Locate the **RESET** button on the ELXM-SW6.

3. Insert the end of a paperclip or similar device into the hole to press the **RESET** button.
4. While pressing the **RESET** button in with a paperclip, apply power to the ELXM-SW6, and continue to hold down the **RESET** button for 10 seconds.
5. This reverts the ELXM-SW6 back to its factory default settings.
6. Log in to the ELXM-SW6 using the default password: **password**.

4.3.2 Resetting to User Defaults

The following steps reset the ELXM-SW6 to a set of default operational settings that were previously loaded using the IH Browser.

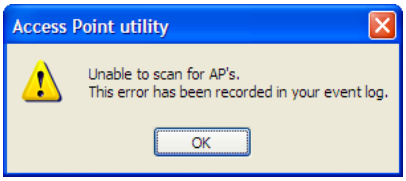
1. Power up the device.
2. Locate the **RESET** button.

3. Once the ELXM-SW6 is running, insert the end of a paperclip or similar device into the hole to press the **RESET** button.
4. After holding the **RESET** button down for 5 seconds an alternating green/red LED pattern will flash on the signal strength and I/O LEDs on the front panel.
5. Release the **RESET** button and the ELXM-SW6 will revert to a User Default configuration that had been previously stored on the ELXM-SW6 using the IH Browser. It will immediately reboot to operate with those User Default settings.

If the Power, I/O and signal LEDs all flash amber 4 times, this indicates that a User Default configuration is not currently present in the ELXM-SW6 and normal operation resumes.

4.4 Unable to Scan for AP's Error Message

The *Unable to scan for AP's* error message may appear in the IH Browser when it attempts to scan and no valid network connection exists on the PC (wired or wireless).



1. Confirm that the PC has at least one active network (LAN) connection. It could be a wired Ethernet connection or a wireless 802.11 connection.
2. Confirm that the network connection has a valid IP address. The network connection might need to have a static IP address assigned to it. Check the IP address of the network connection to determine that one has been assigned.

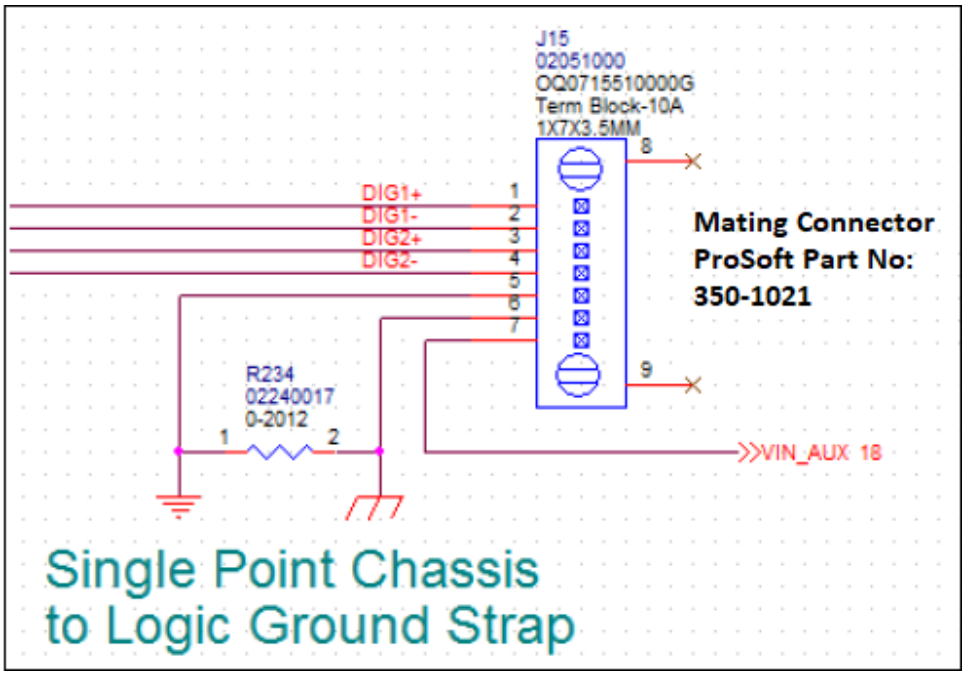
5 Appendix A - Radio Hardware

5.1 Radio Power Requirements

ELXM-SW6's accept voltages between 10 and 30 VDC, with an average power draw of less than 6 Watts. A detachable power connector (ProSoft Technology part number 350-1021) comes with the ELXM-SW6, as shown below. The connector terminal power pins are labeled on the front panel overlay as DC+, DC-, and chassis ground. The DC power wires must be less than 3 meters in length to meet regulatory requirements.

Warning: When wiring the power connector supplied with the ELXM-SW6, be sure to observe the proper polarity markings on the power connector. **Wiring the connector incorrectly can cause serious damage to the ELXM-SW6 which is not covered under the ProSoft Technology warranty**.

The ELXM-SW6 has a plastic enclosure and so a chassis ground internal PCB trace includes the connections listed below. The chassis ground net connects to logic (digital) ground through an installed zero-ohm resistor located next to the input power connector as shown in the following schematic:



Pin	Description
1	Ethernet RJ45 connector metal shield
2	MicroSD socket metal shield
3	Pushbutton switch metal shield
4	All CPU heat sink and board mounting holes
5	Input power connector

The ELXM-SW6 must be installed by trained personnel only, as outlined in the installation instructions provided with each radio.

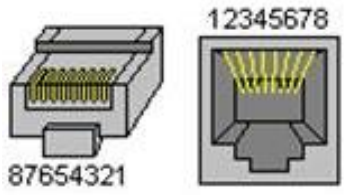
Danger: A solid ground connection should be verified using a meter prior to applying power to the ELXM-SW6. Failing to secure a proper ground could result in serious injury or death because of a lightning strike.

5.2 Ethernet Cable Specifications

- The recommended cable is Category 5 or better. A Category 5 cable has four twisted pairs of wires, which are color-coded and cannot be swapped. The ELXM-SW6 uses only two of the four pairs when running at 10 Mbit/s or 100 Mbit/s speeds. All eight wires are used when running at 1000 Mbit/s speeds.
- Category 5e or better cable is recommended for 1000 Mbit/s speeds.
- The Ethernet port on the module is Auto-Sensing. Use either a standard Ethernet straight-through cable or a crossover cable when connecting the module to an Ethernet hub, a 10/100/1000 Base-T Ethernet switch, or directly to a PC. The ELXM-SW6 detects the cable type and uses the appropriate pins to send and receive Ethernet signals.

5.3 Ethernet Cable Configuration

A diagram of the pin assignments are shown below:



5.4 Straight-Though Cable

RJ-45 Pin	RJ-45 Pin
1 Rx+	1 Tx+
2 Rx-	2 Tx-
3 Tx+	3 Rx+
6 Tx-	6 Rx-

5.5 Crossover Cable

RJ-45 Pin	RJ-45 Pin
1 Rx+	3 Tx+
2 Rx-	6 Tx-
3 Tx+	1 Rx+
6 Tx-	2 Rx-

6 Appendix B - ELXM-SW6 Virtual LAN (VLAN) Functionality

Virtual Local Area Networks (VLANs) are typically used to segment core network components and network access rules. A VLAN provides the equivalent of a wired patch panel through software (packet filtering) rather than hardware (physical wires).

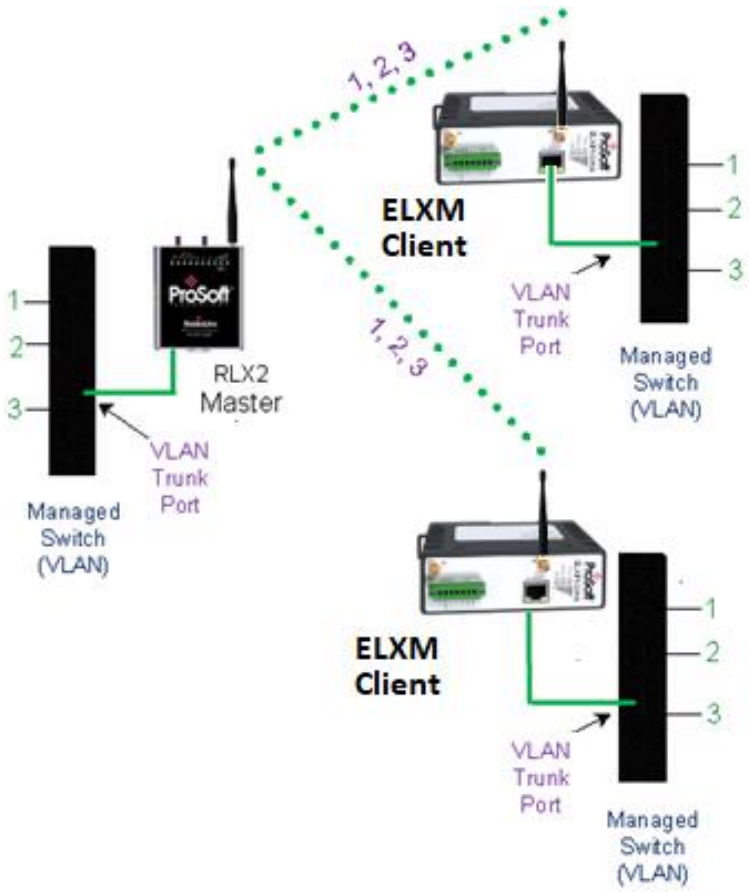
Constraining data to a particular Virtual LAN requires that the ELXM-SW6 tag packets with a VLAN identifier. VLAN tagging simply adds extra information in the packet header of Ethernet frames so VLAN-enabled switches know how to pass along the data.

The ELXM-SW6's (version 33 and later) provide:

- Transparent support of VLAN tags (802.1Q)
- Port/Radio-based VLAN tagging with Managed Switches
- Port/Radio-based VLAN tagging without Managed Switches

6.1 Transparent Support of VLAN Tags (802.1Q)

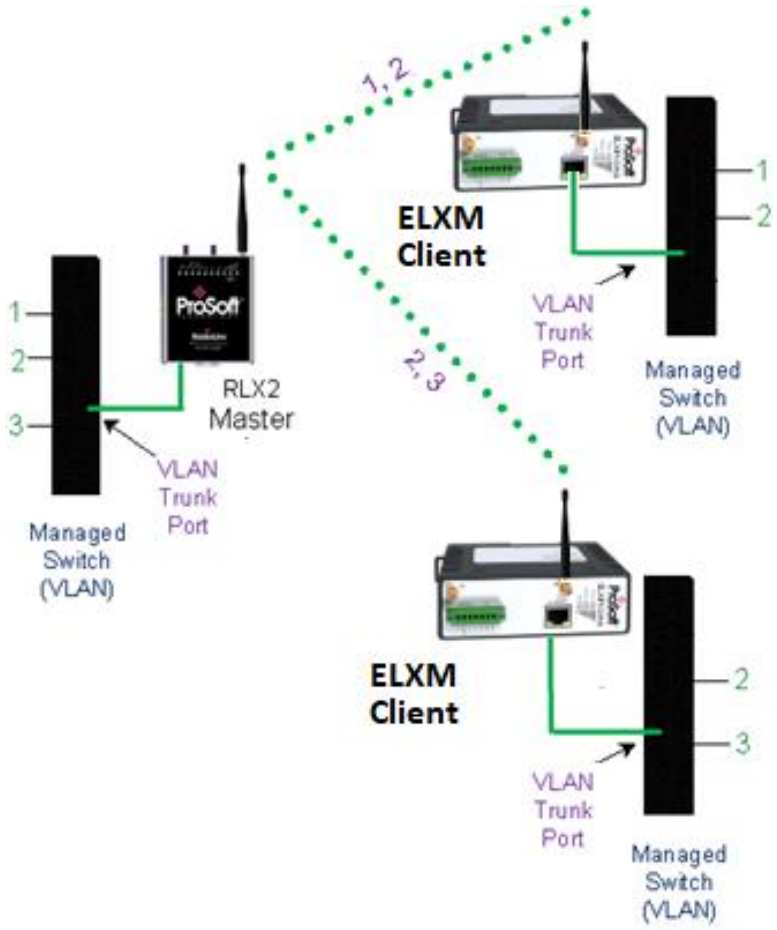
The following provides an example of transparent communication between Managed switches using VLAN trunking. This is achieved by default without any VLAN configuration in the ELXM-SW6.



6.2 Port/Radio-based VLAN Tagging with Managed Switches

In this example, the network has three VLANs (capacity for 15). Each VLAN has access to a Managed Switch pre-configured to assign each VLAN to a specific port. The Radio supporting the Managed Switch passes on the 802.1Q frames. This example shows support for Radio to Radio VLANs using one or more Trunk Links and is achieved with specific configuration of the Radio's VLAN settings.

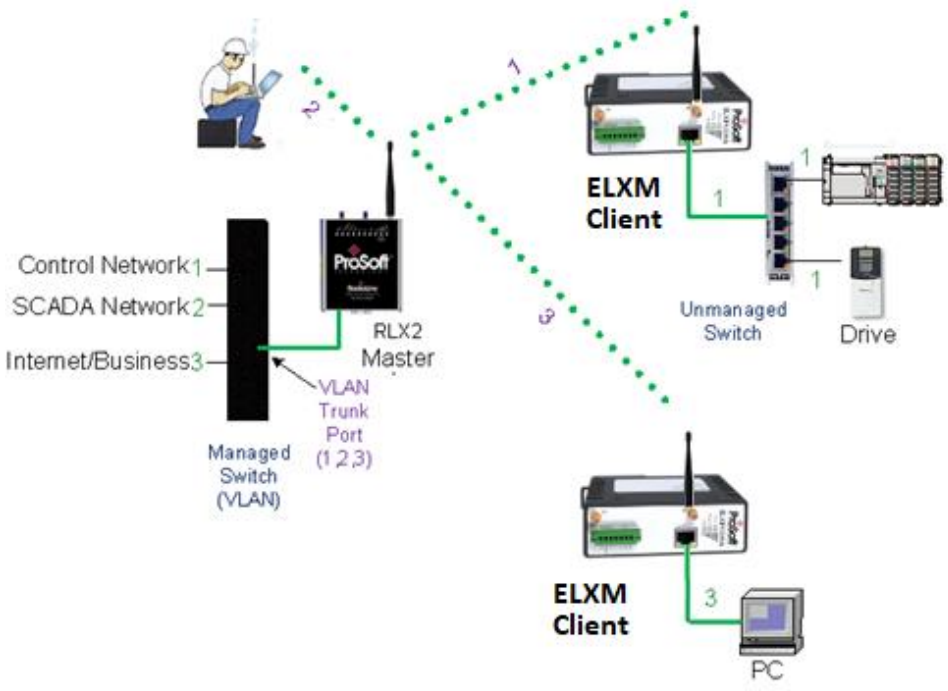
- The 1st remote managed switch only gets VLAN 1 and 2 traffic.
- The 2nd remote managed switch only gets VLAN 2 and 3 traffic.



6.3 Port/Radio-based VLAN Tagging without Managed Switches

In the following example, the network has three VLANs (capacity for 15). Each VLAN has access to a specific Radio port. The Radio supporting the Managed Switch passes on the 802.1Q frames. The wireless network also supports Radio to Radio VLANs using one or more Trunk Links.

- PLC, Drive & HMI communicate on one VLAN on the same subnet.
- Mobile Worker/Laptop communicate with a fixed server on VLAN 2 (separate subnet).



7 Appendix C - Modbus® TCP/IP and EtherNet/IP™ Support

You can get diagnostic and status information from the ELXM-SW6 by querying the ELXM-SW6 using either the Ethernet/IP or Modbus TCP/IP protocols.

7.1 Modbus® TCP/IP Server Support

Use a Modbus TCP/IP client to poll the ELXM-SW6 for diagnostic and status information. The Modbus TCP/IP server in the ELXM-SW6 monitors port 502 and port 2000, and responds to requests from the port eth0 (Ethernet port) or ppp0 (Point-to-Point Protocol). PPP is a data link layer protocol that establishes a connection between two nodes.

The ELXM-SW6 supports up to five concurrent Modbus TCP/IP client connections.

7.1.1 Modbus Memory Map Diagnostic Information

The following table includes the Modbus register addresses used to read the ELXM-SW6 diagnostic and status information.

Name	Data Type	Access	Modbus Register
ELXM-SW6_Diag.SSID	SINT[32]	Read	30001 to 30016
ELXM-SW6_Diag.IPAddress	SINT[4]	Read	30017 to 30018
ELXM-SW6_Diag.MACAddress	SINT[6]	Read	30019 to 30021
ELXM-SW6_Diag.NeworkMode	SINT	Read	30022
ELXM-SW6_Diag.ConnectionState	SINT	Read	30023
ELXM-SW6_Diag.SignalStrength	INT	Read	30024
ELXM-SW6_Diag.Channel	SINT	Read	30025
ELXM-SW6_Diag.WEP	SINT	Read	30026
ELXM-SW6_Diag.Flags	DINT	Read	30027 to 30028
ELXM-SW6_Diag.MasterMACAddress	SINT[6]	Read	30029 to 30031
ELXM-SW6_Diag.HopCount	SINT	Read	30032
ELXM-SW6_DiagStatus	SINT	Read	30033
ELXM-SW6_Diag.NumAssociations	INT	Read	30034
ELXM-SW6_Diag.NumBridgeAssocs	INT	Read	30035
ELXM-SW6_Diag.TxRadioThroughput	INT	Read	30036
ELXM-SW6_Diag.RxRadioThroughput	INT	Read	30037
ELXM-SW6_Diag.Uptime	DINT	Read	30038 to 30039
ELXM-SW6_Diag.LinkTime	DINT	Read	30040 to 30041
ELXM-SW6_Diag.TxPktThput	DINT	Read	30042 to 30043
ELXM-SW6_Diag.RxPktThput	DINT	Read	30044 to 30045
ELXM-SW6_Diag.ModuleName	SINT[32]	Read	30046 to 30061
ELXM-SW6_Diag.ProductName	SINT[32]	Read	30062 to 30077
ELXM-SW6_Diag.ImageVerStr	SINT[28]	Read	30078 to 30091
ELXM-SW6_Diag.tx_good	DINT	Read	30092 to 30093
ELXM-SW6_Diag.rx_good	DINT	Read	30094 to 30095
ELXM-SW6_Diag.tx_bad	DINT	Read	30096 to 30097
ELXM-SW6_Diag.rx_bad	DINT	Read	30098 to 30099
ELXM-SW6_Diag.tx_directed_frames	DINT	Read	30100 to 30101
ELXM-SW6_Diag.tx_multicast_frames	DINT	Read	30102 to 30103

ELXM-SW6_Diag.tx_broadcast_frames	DINT	Read	30104 to 30105
ELXM-SW6_Diag.rx_directed_frames	DINT	Read	30106 to 30107
ELXM-SW6_Diag.rx_multicast_frames	DINT	Read	30108 to 30109
ELXM-SW6_Diag.rx_broadcast_frames	DINT	Read	30110 to 30111
ELXM-SW6_Diag.rx_crc_error	DINT	Read	30112 to 30113

The following registers are available if the firmware in the ELXM-SW6 is *ELXM-SW6_v0038_R or greater.*

Name	Data Type	Access	Modbus Register
ELXM-SW6_Diag.Retries	INT	Read	30114
ELXM-SW6_Diag.Utilization	INT	Read	30115
ELXM-SW6_Diag.ChannelWidth	INT	Read	30116
ELXM-SW6_Diag.NumAntennas	INT	Read	30117
ELXM-SW6_Diag.TxRate	INT	Read	30118
ELXM-SW6_Diag.TxBitRate	INT	Read	30119
ELXM-SW6_Diag.TxBcstRate	INT	Read	30120
ELXM-SW6_Diag.TxMcstRate	INT	Read	30121
ELXM-SW6_Diag.OS_Files	DINT	Read	30122 to 30123
ELXM-SW6_Diag.Wireless_Files	DINT	Read	30124 to 30125
ELXM-SW6_Diag.Config_Files	DINT	Read	30126 to 30127
ELXM-SW6_Diag.Security_Files	DINT	Read	30128 to 30129
ELXM-SW6_Diag.Web_Files	DINT	Read	30130 to 30131
ELXM-SW6_Diag.SD_Card_Files	DINT	Read	30132 to 30133

* Modbus Function Code 4 (Read Input Registers(3X)) is supported.

7.2 EtherNet/IP™ Server Support

The following table contains the CIP™ object definitions used to read the ELXM-SW6 diagnostic and status information.

Class ID: 0xA1 (161)
Number of Instances: 1

CIP Data Tag Name	Data Type	Access
ELXM-SW6_Diag.SSID	SINT[32]	Read
ELXM-SW6_Diag.IPAddress	SINT[4]	Read
ELXM-SW6_Diag.MACAddress	SINT[6]	Read
ELXM-SW6_Diag.NetworkMode	SINT	Read
ELXM-SW6_Diag.ConnectionState	SINT	Read
ELXM-SW6_Diag.SignalStrength	INT	Read
ELXM-SW6_Diag.Channel	SINT	Read
ELXM-SW6_Diag.WEP	SINT	Read
ELXM-SW6_Diag.Flags	DINT	Read
ELXM-SW6_Diag.MasterMACAddress	SINT[6]	Read
ELXM-SW6_Diag.HopCount	SINT	Read
ELXM-SW6_Diag.Status	SINT	Read
ELXM-SW6_Diag.NumAssociations	INT	Read
ELXM-SW6_Diag.NumBridgeAssocs	INT	Read
ELXM-SW6_Diag.TxRadioThroughput	INT	Read
ELXM-SW6_Diag.RxRadioThroughput	INT	Read
ELXM-SW6_Diag.Uptime	DINT	Read
ELXM-SW6_Diag.Linktime	DINT	Read
ELXM-SW6_Diag.TxPktThput	DINT	Read
ELXM-SW6_Diag.RxPktThput	DINT	Read
ELXM-SW6_Diag.ModuleName	SINT[32]	Read
ELXM-SW6_Diag.ProductName	SINT[32]	Read
ELXM-SW6_Diag.ImageVerStr	SINT[28]	Read
ELXM-SW6_Diag.tx_good	DINT	Read
ELXM-SW6_Diag.rx_good	DINT	Read
ELXM-SW6_Diag.tx_bad	DINT	Read
ELXM-SW6_Diag.rx_bad	DINT	Read
ELXM-SW6_Diag.tx_directed_frames	DINT	Read
ELXM-SW6_Diag.tx_multicast_frames	DINT	Read
ELXM-SW6_Diag.tx_broadcast_frames	DINT	Read
ELXM-SW6_Diag.rx_directed_frames	DINT	Read
ELXM-SW6_Diag.rx_multicast_frames	DINT	Read
ELXM-SW6_Diag.rx_broadcast_frames	DINT	Read
ELXM-SW6_Diag.rx_crc_err	DINT	Read

Class ID: 0xA2 (162) - ELXM-SW6 Info Extended
Number of Instances: 1
Available from ELXM-SW6's with firmware *ELXM-SW6_v0038_R* or later.

CIP Data Tag Name	Data Type	Access
ELXM-SW6_Diag.SSID	SINT[32]	Read
ELXM-SW6_Diag.IPAddress	SINT[4]	Read
ELXM-SW6_Diag.MACAddress	SINT[6]	Read
ELXM-SW6_Diag.NetworkMode	SINT	Read
ELXM-SW6_Diag.ConnectionState	SINT	Read
ELXM-SW6_Diag.SignalStrength	INT	Read
ELXM-SW6_Diag.Channel	SINT	Read
ELXM-SW6_Diag.WEP	SINT	Read
ELXM-SW6_Diag.Flags	DINT	Read
ELXM-SW6_Diag.MasterMACAddress	SINT[6]	Read
ELXM-SW6_Diag.HopCount	SINT	Read
ELXM-SW6_Diag.Status	SINT	Read
ELXM-SW6_Diag.NumAssociations	INT	Read
ELXM-SW6_Diag.NumBridgeAssocs	INT	Read
ELXM-SW6_Diag.TxRadioThroughput	INT	Read
ELXM-SW6_Diag.RxRadioThroughput	INT	Read
ELXM-SW6_Diag.Uptime	DINT	Read
ELXM-SW6_Diag.Linktime	DINT	Read
ELXM-SW6_Diag.TxPktThput	DINT	Read
ELXM-SW6_Diag.RxPktThput	DINT	Read
ELXM-SW6_Diag.ModuleName	SINT[32]	Read
ELXM-SW6_Diag.ProductName	SINT[32]	Read
ELXM-SW6_Diag.ImageVerStr	SINT[28]	Read
ELXM-SW6_Diag.tx_good	DINT	Read
ELXM-SW6_Diag.rx_good	DINT	Read
ELXM-SW6_Diag.tx_bad	DINT	Read
ELXM-SW6_Diag.rx_bad	DINT	Read
ELXM-SW6_Diag.tx_directed_frames	DINT	Read
ELXM-SW6_Diag.tx_multicast_frames	DINT	Read
ELXM-SW6_Diag.tx_broadcast_frames	DINT	Read
ELXM-SW6_Diag.rx_directed_frames	DINT	Read
ELXM-SW6_Diag.rx_multicast_frames	DINT	Read
ELXM-SW6_Diag.rx_broadcast_frames	DINT	Read
ELXM-SW6_Diag.rx_crc_err	DINT	Read
ELXM-SW6_Diag.Retries	SINT	Read
ELXM-SW6_Diag.Utilization	SINT	Read
ELXM-SW6_Diag.ChannelWidth	SINT	Read
ELXM-SW6_Diag.NumAntennas	SINT	Read
ELXM-SW6_Diag.TxRate	INT	Read
ELXM-SW6_Diag.TxBitRate	INT	Read
ELXM-SW6_Diag.TxBcastRate	INT	Read
ELXM-SW6_Diag.TxMcstRate	INT	Read
ELXM-SW6_Diag.Reserved1	DINT	Read
ELXM-SW6_Diag.Reserved2	DINT	Read
ELXM-SW6_Diag.Reserved3	DINT	Read
ELXM-SW6_Diag.Reserved4	DINT	Read
ELXM-SW6_Diag.Reserved5	DINT	Read
ELXM-SW6_Diag.Reserved6	DINT	Read

ELXM-SW6_Diag.Reserved7	DINT	Read
ELXM-SW6_Diag.Reserved8	DINT	Read
ELXM-SW6_Diag.Reserved9	DINT	Read
ELXM-SW6_Diag.Reserved10	DINT	Read
ELXM-SW6_Diag.Reserved11	DINT	Read
ELXM-SW6_Diag.Reserved12	DINT	Read
ELXM-SW6_Diag.Reserved13	DINT	Read
ELXM-SW6_Diag.Reserved14	DINT	Read
ELXM-SW6_Diag.Reserved15	DINT	Read
ELXM-SW6_Diag.Reserved16	DINT	Read

Class ID: 0xA3 (163) - File CRC Signatures
Number of Instances: 1

Available from ELXM-SW6's with firmware *ELXM-SW6_v0038_R* or later.

CIP Data Tag Name	Data Type	Access
ELXM-SW6_CRC.OS_Sig	DINT	Read
ELXM-SW6_CRC.Wireless_Sig	DINT	Read
ELXM-SW6_CRC.Config_Sig	DINT	Read
ELXM-SW6_CRC.Security_Sig	DINT	Read
ELXM-SW6_CRC.Web_Sig	DINT	Read
ELXM-SW6_CRC.SDCard_Sig	DINT	Read
ELXM-SW6_CRC.Rsvd1	DINT	Read
ELXM-SW6_CRC.Rsvd2	DINT	Read
ELXM-SW6_CRC.Rsvd2	DINT	Read
ELXM-SW6_CRC.Rsvd3	DINT	Read
ELXM-SW6_CRC.Rsvd4	DINT	Read
ELXM-SW6_CRC.Rsvd5	DINT	Read
ELXM-SW6_CRC.Rsvd6	DINT	Read
ELXM-SW6_CRC.Rsvd7	DINT	Read
ELXM-SW6_CRC.Rsvd8	DINT	Read
ELXM-SW6_CRC.Rsvd9	DINT	Read
ELXM-SW6_CRC.Rsvd10	DINT	Read
ELXM-SW6_CRC.Rsvd11	DINT	Read
ELXM-SW6_CRC.Rsvd12	DINT	Read
ELXM-SW6_CRC.Rsvd13	DINT	Read
ELXM-SW6_CRC.Rsvd14	DINT	Read

8 Appendix D - AP Channel-Frequency Table

The following table includes the channels/frequencies available in each ELXM-SW6 when in AP mode. Note that ELXM-SW6's configured for FCC and ETSI regulatory domains do not have the same channels available. Also, some channels may have usage or power restrictions (for example, indoor or outdoor) in some locations.

Channel Number	Center Frequency (MHz)	FCC ELXM-SW6-A	ETSI ELXM-SW6-E
1	2412	✓	✓
2	2417	✓	✓
3	2422	✓	✓
4	2427	✓	✓
5	2432	✓	✓
6	2437	✓	✓
7	2442	✓	✓
8	2447	✓	✓
9	2452	✓	✓
10	2457	✓	✓
11	2462	✓	✓
12	2467		✓
13	2472		✓
36	5180	✓	✓
40	5200	✓	✓
44	5220	✓	✓
48	5240	✓	✓
52 (DFS)	5260	Only Client modes	Only Client modes
56 (DFS)	5280	Only Client modes	Only Client modes
60 (DFS)	5300	Only Client modes	Only Client modes
64 (DFS)	5320	Only Client modes	Only Client modes
100 (DFS)	5500	Only Client modes	Only Client modes
104 (DFS)	5520	Only Client modes	Only Client modes
108 (DFS)	5540	Only Client modes	Only Client modes
112 (DFS)	5560	Only Client modes	Only Client modes
116 (DFS)	5580	Only Client modes	Only Client modes
120 (DFS)	5600	Only Client modes	Only Client modes
124 (DFS)	5620	Only Client modes	Only Client modes
128 (DFS)	5640	Only Client modes	Only Client modes
132 (DFS)	5660	Only Client modes	Only Client modes
136 (DFS)	5680	Only Client modes	Only Client modes
140 (DFS)	5700	Only Client modes	Only Client modes
149	5745	✓	
153	5765	✓	
157	5785	✓	
161	5805	✓	
165	5825	✓	

9 Appendix E - FCC Emission Regulations

The charts in this section show the maximum emissions allowed for the FCC in the United States. These data should only be considered guidelines. Consult official FCC documents for the latest official regulations.

In the 2.4 GHz band, the maximum Equivalent Isotropically Radiated Power (EIRP) is 4W for multipoint links: that is, radios with omnidirectional antennas. Point-to-Point links using directional antennas are allowed higher EIRP.

9.1 2.4 GHz Band, Point-To-Multipoint

Maximum Power From Radio		Maximum Antenna Gain	Maximum EIRP	
dBm	**mW**	**dBi**	**dBm**	**W**
30	1000	6	36	4
27	500	9	36	4
24	250	12	36	4
21	125	15	36	4
18	63	18	36	4
15	32	21	36	4
12	16	24	36	4

9.2 2.4 GHz Band, Point-To-Point

Maximum Power From Radio		Maximum Antenna Gain	Maximum EIRP	
dBm	**mW**	**dBi**	**dBm**	**W**
30	1000	6	36	4.0
29	800	9	38	6.3
28	630	12	30	10.0
27	500	15	42	16.0
26	400	18	44	25.0
25	316	21	46	39.8
24	250	24	48	63.0
23	200	27	50	100.0
22	160	30	52	158.0

The FCC states that for every 1 dBi power reduction in the ELXM-SW6's transmitter output, the antenna gain may be increased by 3 dB.

9.3 5 GHz Bands, Point-To-Multipoint

5 GHz Band	Frequency Range (GHz)	Channels	Permitted Location	Maximum Power from Radio		Maximum EIRP	
				dBm	mW	dBm	W
UNII	5.15 to 5.25	36, 40, 44, 48	Indoor or Outdoor	30	1000	36	4
UNII-2	5.25 to 5.35	52, 56, 60, 64	Indoor or Outdoor	24	250	30	1
UNII-2 Extended	5.470 to 5.725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor or Outdoor	24	250	30	1
UNII-3	5.725 to 5.825	149, 153, 157, 161, 165	Typical Outdoor	30	1000	36	4

9.4 5 GHz Bands, Point-To-Point

5 GHz Band	Frequency Range (GHz)	Channels	Permitted Location	Maximum Power from Radio		Maximum EIRP	
				dBm	mW	dBm	W
UNII	5.15 to 5.25	36, 40, 44, 48	Indoor or Outdoor	30	1000	53	200
UNII-2	5.25 to 5.35	52, 56, 60, 64	Indoor or Outdoor	24	250	30	1
UNII-2 Extended	5.470 to 5.725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor or Outdoor	24	250	30	1
UNII-3	5.725 to 5.825	149, 153, 157, 161, 165	Indoor or Outdoor	30	1000	No limit	No limit

10 Appendix F - Detailed Radio Specifications

10.1 ELXM-SW6 Detailed Specifications

10.1.1 Radio

Specification	Frequency	Channel
Frequency Band (Varies by country)	2.412 GHz to 2.462 GHz (FCC) 2.412 GHz to 2.472 GHz (ETSI)	1 to 11 1 to 13
	5.150 GHz to 5.250 GHz (FCC/ETSI) 5.250 GHz to 5.350 GHz (FCC/ETSI)* 5.450 GHz to 5.725 GHz (FCC/ETSI)* 5.725 GHz to 5.850 GHz (FCC/ETSI) * DFS channels with RADAR detection	36 to 48 52 to 64* 100 to 140* 149 to 165
Wireless Standards	802.11ax, 802.11ac, 802.11n, 802.11a, 802.11g, 802.11h (DFS), 802.11i (Security), 802.11e (QoS) 802.112Q (VLAN), IGMPv2	
Transmit Power / RF chain +/- 2 dB (Programmable) *Subject to Regional Regulatory Limits	16 dBm @ MCS0, (802.11ax/ac/an - 5 GHz) 17.5 dBm @ MCS0, (802.11ax/gn - 2.4 GHz) 12 dBm @ MCS8, (802.11ax/ac - 5 GHz) 14 dBm @ MCS7, (802.11ax/gn - 2.4 GHz) 11.5 dBm @ MCS11, (802.11ax - 2.4 GHz)	
	Antenna Impact: 2 Antennas: Add 3 dB to values above	
Channel data rates (802.11ax)	MCS0 through MCS11, 20MHz, 40MHz or 80MHz channels with 1 or 2 Streams Rates shown for largest Guard Interval (GI=3.2usec)	

20 MHz Channels	40 MHz Channels	80 MHz Channels	Rate	Streams
7.3 Mbps	14.6 Mbps	30.6 Mbps	MCS0	1 Stream
121.9 Mbps	243.8 Mbps	510.4 Mbps	MCS11	
14.6 Mbps	29.3 Mbps	61.3 Mbps	MCS0	2 Streams
243.8 Mbps	487.5 Mbps	1020.8 Mbps	MCS11	

Receiver Sensitivity (Typical, 1x1 chain)	-95 dBm @ MCS0, (802.11ax/n, 5 GHz) -92.5 dBm @ MCS0, (802.11ax/n, 2.4 GHz) -77 dBm @ MCS7, (802.11ax/n, 5 GHz) -72.5 dBm @ MCS7, (802.11ax/n, 2.4 GHz) -66 dBm @ MCS11, (802.11ax, 5 GHz) -63 dBm @ MCS11, (802.11ax, 2.4 GHz)
Security	WPA2 Personal/Enterprise – 802.11i AES Legacy WPA support

10.1.2 Physical

Specification	Description
Enclosure	Plastic - can be either DIN rail or panel mounted.
Size (H x W x D)	130 x 40 x 100 mm (with DIN rail clip) 5.11 x 1.57 x 3.93 in 122 x 40 x 100 mm (without DIN rail clip) 4.80 x 1.57 x 3.93 in
Shock (panel mount)	IEC 60068 2-27 (15g, 3-Axis)
Vibration (panel mount)	IEC 60068 2-6 (5g, 10Hz to 150Hz)
Ethernet Port	(1) 10/100/1000 Base-T connector, shielded RJ45 IEEE 802.3, 802.3u, 802.3x, 802.3ab, 802.3ac
Antenna Port	(2) RP-SMA connector
Personality Module	Industrial microSD Memory Module
Weight	0.6 lbs (0.27 kg)

10.1.3 Environmental

Specification	Description
Operating Temperature	-4°F to +149°F (-20°C to +65°C)
Humidity	Up to 100% RH, with no condensation
External Power	10 to 30 VDC
Peak Power Consumption	< 6W

10.1.4 Agency Approvals & Certifications

Visit www.prosoft-technology.com for current wireless approval information.

11 Glossary of Terms

Term	Description
802.11	A group of wireless specifications developed by the IEEE. It details a wireless interface between devices to transport packet traffic.
802.11a	Operates in the 5 GHz frequency range with a maximum 54 Mbit/sec signaling rate.
802.11b	Operates in the most used 2.4 GHz Industrial, Scientific, and Measurement (ISM) band. Provides signaling rates of up to 11 Mbit/sec using CCK modulation.
802.11g	Similar to 802.11b but supports signaling rates of up to 54 Mbit/sec using OFDM modulation. Operates in the heavily used 2.4 GHz ISM band.
802.11i	Sometimes called Wi-Fi Protected Access 2 (WPA 2). WPA 2 exclusively uses the 128-bit and above Advanced Encryption Standard (AES), along with 802.1x authentication and key management features.
802.11n	Uses higher modulation rates and packet aggregation to raise effective WLAN throughput to more than 100 Mbit/sec.
Access Point	A generic term for an 802.11 radio that "attaches" other 802.11 (clients) to a wired network. Some access points (APs) can also bridge to other APs
Ad hoc Mode	Wireless network framework in which devices can communicate directly with one another without using an access point or a connection to a regular network. ELXM-SW6's do not support Ad hoc mode.
AES	Advanced Encryption Standard. New standard for encryption adopted by the U.S. government for secure communications.
Amplifier	A device connected to an antenna that increases the signal strength and amplifies weak incoming signals.
Antenna	A device connected to a wireless transceiver that concentrates transmitted and received radio waves to increase signal strength and thus the effective range of a wireless network.
ASCII	American Standard Code for Information Interchange. A communication mode in which each eight-bit byte in a message contains one ASCII character code. ASCII characters (or hexadecimal characters) are sometimes used as a key to encrypt data and ensure its secure transmission.
Association	Process whereby two 802.11 radios establish communications with each other. Requirements for communication include the same SSID (network names) and encryption settings.
Authenticate	The process of confirming the identity of someone connecting to a network.
Authentication Server	A back-end database server that confirms the identity of a supplicant to an authenticator in an 802.1x-authenticated network.
Band	Another term for spectrum used to indicate a particular set of frequencies. Wireless networking protocols work in either the 2.4 GHz or the 5 GHz bands.
Bridging Client, Radio Mode	A radio in Bridging Client mode can connect to any Access Point and can support one multiple Ethernet device but can only bridge IP-based traffic. See also Repeater, Radio Mode.
CACT	CACT is an acronym for Channel Availability Check Time, a parameter used in DFS channel selection. During DFS when a radio changes channels, it must listen for the CACT on the new channel before beginning operations. For most channels the CACT is 60 seconds.
Channel	One portion of the available radio spectrum that all devices on a wireless network use to communicate. Changing the channel on the access point/router can help reduce interference.
dBi	Decibels referenced to an ideal isotropic radiator in free space; frequently used to express antenna gain

dBm	Decibels referenced to one milliwatt (mW); an absolute unit used to measure signal power (transmit) power output or received signal strength)
DCE	Data communications equipment. A modem, for example.
Decibel (dB)	A measure of the ratio between two signal levels; used to express gain (or loss) in a system.
Default Gateway	The IP address of a network router where data is sent if the destination IP address is outside the local subnet. The gateway is the device that routes the traffic from the local area network to other networks such as the Internet.
Device-to-Device Network (Peer-to-Peer Network)	Two or more devices that connect using wireless network devices without the use of a centralized wireless access point. Also known as a peer-to-peer network.
DFS	DFS stands for Dynamic Frequency Selection, a requirement for operation on certain frequencies in the 5 GHz band in many countries. When a radio operates on a DFS frequency, it must sense the presence of radar and automatically change to another channel if radar is detected.
DHCP	The dynamic host configuration protocol is an Internet protocol, similar to BootP, for automating the configuration of computers that use TCP/IP. DHCP can be used to automatically assign IP addresses, to deliver IP stack configuration parameters, such as the subnet mask and default router, and to provide other configuration information, such as the addresses for printer, time, and news servers.
Direct Sequence Spread Spectrum	A modulation mechanism that spreads the signal for a wide band, allowing reception even for overlapping data signals. 802.11b uses DSSS modulation.
Directional Antenna	Transmits and receives radio waves in a single direction.
Diversity Antenna	An antenna system that uses multiple antennas to reduce interference and maximize reception and transmission quality.
DTE	Data Terminal Equipment, for example, a computer or terminal.
Dual Band	A device that is capable of operating in two frequency bands. On a wireless network, dual-band devices are capable of operating in both the 2.4 GHz (802.11b/g) and 5 GHz (802.11a) bands.
EAP	Extensible Authentication Protocol. A protocol that provides an authentication framework for both wireless and wired Ethernet enterprise networks.
EIRP	Equivalent isotropically radiated power (EIRP) is the amount of power that would have to be emitted by an isotropic antenna (that evenly distributes power in all directions and is a theoretical construct) to produce the peak power density observed in the direction of maximum antenna gain.
Encryption	Method of scrambling data so that only the intended viewers can decipher and understand it.
Firmware	Firmware is the embedded software code that that runs in hardware containing a CPU (like the BIOS in a personal computer). This is distinguished from the IH Browser software that is installed on the Configuration PC.
Fresnel Zone	An elliptical area on either side of the straight line of sight that must also be clear for a long-range wireless network to work.
Full-Duplex	A communications circuit or system designed to simultaneously transmit and receive two different streams of data. Telephones are an example of a full-duplex communication system. Both parties on a telephone conversation can talk and listen at the same time. If both talk at the same time, their two signals are not corrupted.
Gain, Antenna	The amount by which an antenna concentrates signal strength in a wireless network.
Gateway	In wireless terms, a gateway is an access point with additional software capabilities such as providing NAT and DHCP and access to a Wide Area network (WAN), Internet or another main network.

Guard Interval (GI)	An interval of time between data symbols during transmission. The guard interval time for 802.11a/b/g systems is fixed at 800 microseconds. 802.11n devices can also use a 400-microsecond guard interval, falling back to 800 microseconds if excessive data corruption is detected.
Half-Duplex	A communications circuit or system designed to transmit and receive data, but not both simultaneously. CB or walkie-talkie radios are an example of a half-duplex communication system. Either parties on a radio conversation may talk or listen; but both cannot talk at the same time without corrupting each other's signal. If one operator is sending, the other must be receiving to have successful communication.
Hz	Hertz. The international unit for measuring frequency equivalent to the older unit of cycles per second. One megahertz (MHz) is one million hertz. One gigahertz (GHz) is one billion hertz. The standard US electrical power frequency is 60 Hz. 802.11a devices operate in the 5 GHz band; 802.11b and g devices operate in the 2.4 GHz band.
IEEE	Institute of Electrical and Electronics Engineers, Inc. IEEE is a professional organization with members in over 175 countries and is an authority in technical areas such as computer engineering and telecommunications. IEEE developed the 802.11 specifications.
IP Address	A 32-bit identification number for each node on an Internet Protocol network. These addresses are represented as four sets of 8-bit numbers (numbers from 0 to 255), separated by periods ("dots"). Networks using the TCP/IP protocol route messages based on the IP address of the destination. Each number can be 0 to 255. For example, 192.168.0.100 could be an IP address. Each node on the network must have a unique IP address.
Key	A set of information (often from 40 to as much as 256 bits in size) that is used as a seed to an encryption algorithm to encrypt (scramble) data. Ideally, the key must also be known by the receiver to decrypt the data.
LAN	Local Area Network. A system of connecting PCs and other devices within the same physical proximity for sharing resources such as internet connections, printers, files, and drives. When Wi-Fi is used to connect the devices, the system is known as a wireless LAN or WLAN.
LED	Light-emitting diode.
Line of Sight (LoS)	A clear line from one antenna to another in a long-range wireless network.
MAC ID	Media Access Control address. Every device has its own MAC address which is a unique identifier used to unambiguously identify the source and destination of any packet on the network.
Mbps	Megabits per second, or a million bits per second. A measure of data rate.
Megahertz	A measure of electromagnetic wave frequency equal to one million hertz. Often abbreviated as MHz and used to specify the radio frequency used by wireless devices.
MIC	Message Integrity Check. One of the elements added to the TKIP standard. A signature is added by each radio on each packet it transmits. The signature is based on the data in the packet, a 64-bit value (key) and the MAC address of the sender. The MIC allows the receiving radio to verify (check) that the data is not forged or altered.
MIMO	Multiple Input Multiple Output refers to using multiple antennas in a Wi-Fi device to improve performance and throughput. MIMO technology takes advantage of a characteristic called multipath, which occurs when a radio transmission starts out at Point A and the reflects off or passes through surfaces or objects before arriving, via multiple paths, at Point B. MIMO technology uses multiple antennas to collect and organize signals arriving via these paths.

Modbus	The Modbus protocol provides the internal standard that the MODICON® controllers use for parsing messages. During communications on a Modbus network, the protocol determines how each controller knows its device address, recognizes a message addressed to it, determines the kind of action to be taken, and extracts any data or other information contained in the message. If a reply is required, the controller constructs the reply message and sends it using Modbus protocol.
Modem	MOdulator-DEModulator, a device that converts digital signals to analog signals and vice-versa. Analog signals can be transmitted over communications links such as telephone lines.
Network	A series of stations or nodes connected by some type of communication medium. A network may consist of a single link or multiple links.
Node	An address or software location on the network.
Non-Occupancy Period	The time during which a radio cannot return to a frequency where radar was detected. This time is typically 30 minutes. Typically, a radio will not return to a channel where radar was previously detected unless absolutely necessary.
Null Modem Cable	A specialty cross-communication cable with female connectors on each end used for direct connection between DTE devices when no modems are present. Commonly used as a quick and inexpensive way to transfer files between two PCs without installing a dedicated network card in each PC.
Panel Antenna	An antenna type that radiates in only a specific direction. Panel antennas are commonly used for point-to-point situations. Sometimes called Patch antennas.
Parabolic Antenna	An antenna type that radiates a very narrow beam in a specific direction. Parabolic antennas offer the highest gain for long-range point-to-point situations.
Peer-to-Peer Network	Each radio in a Peer-to-Peer network can receive data from, and transmit data to, any other radio in the network.
Point-to-Multipoint	A wireless network in which one device (the access point) serves multiple other devices associated to it.
Point-to-Point Network	A network consisting of a single AP radio and a single Remote radio.
Poll	A method of electronic communication.
Power Supply	A device that supplies electrical power to the I/O chassis containing the processor, coprocessor, or other modules.
Protocol	The language or packaging of information that is transmitted between nodes on a network.
QoS	Quality of Service. Required to support wireless multimedia applications and advanced traffic management. QoS enables Wi-Fi access points to prioritize traffic and optimize the way shared network resources are allocated among different applications.
Range	The distance covered by a wireless network radio device. Depending on the environment and the type of antenna used, Wi-Fi signals can have a range of up to a several miles.
Repeater	A Repeater is a device used to extend the range of a Wi-Fi signal. Placed at the edge of signal reception, a repeater can receive and re-transmit the signal.
Repeater, Radio Mode	The ELXM-SW6 in Repeater mode can only connect to other ProSoft Technology radios but can bridge any number of Ethernet network devices attached to it. It also simultaneously functions as an access point, allowing other wireless devices to associate to it. See also Client, Radio Mode.
RS-232	Recommended Standard 232; the standard for serial binary signals between DTE and DCE devices.
Sector Antenna	An antenna type that radiates in only a specific direction. Multiple sector antennas are commonly used in point-to-multipoint situations.
Signal Diversity	A process by which two antennas are used to send and receive, combining their results for better effect.

Signal Loss	The amount of signal strength that's lost in antenna cable, connectors, and free space. Signal loss is measured in decibels (dB). Also referred to as gain loss.
Signal Strength	The strength of the radio waves received at a wireless device.
Site Survey	A comprehensive facility study performed by network managers to ensure that planned service levels will be met when a new wireless LAN or additional WLAN segments to an existing network are deployed. Site surveys are usually performed by a radio frequency engineer and used by systems integrators to identify the optimum placement of access points to ensure that planned levels of service are met. Site surveys are sometimes conducted following the deployment to ensure that the WLAN is achieving the necessary level of coverage. Site surveys can also be used to detect rogue access points.
Spectrum	A range of electromagnetic frequencies.
Spread Spectrum	A form of wireless communication in which a signal's frequency is deliberately varied. This increases bandwidth and lessens the chances of interruption or interception of the transmitted signal.
SSID	Service Set Identifier is a sequence of characters unique to a specific network or network segment that's used by the network and all attached devices to identify themselves and allow devices to connect to the correct network when one or more than one independent network is operating in nearby areas.
Subnet Mask	A mask used to determine what subnet an IP address belongs to. An IP address has two components: the network address, and the host (node or device) address; for example, the IP address 150.215.017.009. Assuming this is part of a Class B network (with a subnet mask of 255.255.0.0), the first two numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.
TKIP	Temporal Key Integrity Protocol. A wireless security encryption mechanism in Wi-Fi Protected Access (WPA).
UART	Universal Asynchronous Receiver/Transmitter
WDS	Wireless Distribution System. Enables access points to communicate with one another to extend the range of a wireless networks. Used in 802.11g based access points.
WEP	Wired-Equivalent Privacy protocol was specified in the original IEEE 802.11 standard to provide a WLAN with a minimal level of security and privacy comparable to a typical wired LAN, using data encryption.
Wi-Fi	A certification mark managed by a trade group called the Wi-Fi Alliance. Wi-Fi certification encompasses numerous standards including 802.11a, 802.11b, 802.11g, WPA, and more. Equipment must pass compatibility testing to receive the Wi-Fi mark.
Wi-Fi CERTIFIED™	The certification standard designating IEEE 802.11-based wireless local area network (WLAN) products that have passed interoperability testing requirements developed and governed by the Wi-Fi alliance.
Wi-Fi Interoperability Certificate	A statement that a product has passed interoperability testing and will work with other Wi-Fi CERTIFIED products.
Wi-Fi Protected Setup	Wi-Fi Protected Setup™ (previously called Wi-Fi Simple Config) is an optional certification program developed by the Wi-Fi alliance designed to ease set up of security enabled Wi-Fi networks in the home and small office environment. Wi-Fi Protected Setup supports methods (pushing a button or entering a PIN into a wizard-type application) that are familiar to most consumers to configure a network and enable security.
Wireless Gateway	A term used to differentiate between an access point and a more-capable device that can share an internet connection, serve DHCP, and bridge between wired and wireless networks.
Wireless Network	A network of connected using a centralized wireless access point.

WLAN	Wireless Local Area Network. A type of local area network in which data is sent and received via high-frequency radio waves rather than cables or wires.
WPA	Wi-Fi Protected Access is a data encryption specification for 802.11 wireless networks that replaces the weaker WEP. It improves on WEP by using dynamic keys, Extensible Authentication Protocol to secure network access, and an encryption method called Temporal Key Integrity Protocol (TKIP) to secure data transmissions.
WPA2	An enhanced version of WPA. It is the official 802.11i standard. It uses Advanced Encryption Standard instead of TKIP. AES supports 128-bit, 192-bit, and 256-bit encryption keys.
Yagi Antenna	An antenna type that radiates in only a specific direction. Yagi antennas are used in point-to-point situations.

12 Support, Service, and Warranty

12.1 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

12.2 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