ProSoft® TECHNOLOGY
A BELDEN BRAND

Where Automation Connects.



ELXM-SW6 Series

ProLinx Edge™ Mini

September 15, 2026

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 Series User Manual
For Public Use.

September 15, 2026

ProSoft Technology®, is a registered copyright of ProSoft Technology, Inc. All other brand or product names are or may be trademarks of, and are used to identify products and services of, their respective owners.

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.

© 2026 ProSoft Technology. All Rights Reserved.



For professional users in the European Union

If you wish to discard electrical and electronic equipment (EEE), please contact your dealer or supplier for further information.



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

Agency Approvals and Certifications

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

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 INSURE 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."

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.

Contents

1 Start Here 9

1.1 Before You Begin....9
1.2 About This Manual....9
1.3 About ELXM-SW6 Industrial Hotspot Products....9
1.3.1 Product Overview....9
1.3.2 General Features....10
1.3.3 Antenna Port Connections....11
1.4 Package Contents....12
1.4.1 ELXM-SW6....12
1.5 Installing the Industrial Hotspot Browser....13
1.5.1 IH Browser System Requirements....13
1.5.2 Installing IH Browser Software....13
1.5.3 Starting the IH Browser....13

2 ELXM-SW6 Series Quick Setup 14

2.1 Preparing the Configuration Environment....14
2.2 Making Power and Data Connections....15
2.2.1 ELXM-SW6 Radio Connections....15
2.3 Power-Up....16
2.4 Using the IH Browser to Configure the ELXM-SW6....16
2.4.1 Viewing the Radios in the IH Browser....16
2.4.2 Refreshing the Display in the IH Browser....17
2.4.3 Setting the Radio IP Address in the IH Browser....17
2.4.4 Assigning a Temporary IP Address....17
2.5 Configuring an ELXM-SW6 - Getting Started....19
2.5.1 Connecting to the Radio Configuration Interface....19
2.5.2 Configuring a Bridging Radio....23
2.5.3 Configuring a Bridging Client Radio....25
2.5.4 Configuring a Client Radio....26
2.5.5 Configuring as Soft Access Point (Soft AP)....28
2.6 Viewing an ELXM-SW6 Configuration....31
2.7 Replacing an Existing ELXM-SW6....31

3 Configuring a Radio - Detailed Configuration 32

3.1 Connecting to the Radio Configuration Interface....32
3.1.1 Read-Only Fields....33
3.1.2 Configuration Help....34
3.1.3 Apply Changes....37
3.1.4 Cancelling Changes....38
3.1.5 Factory Defaults....38
3.1.6 User Defaults....38
3.2 Viewing Radio Status....39
3.2.1 Viewing Available Parents for a Radio....41
3.3 Configuring Basic Settings....43
3.3.1 Basic Wireless Settings....44
3.3.2 Wireless Security Settings....47
3.3.3 Access Settings....52
3.4 Configuring Advanced Settings....53
3.4.1 Advanced Wireless Settings....54

3.4.2 Roam Control Settings 59
3.4.3 RF Medium Settings 61
3.4.4 Personality Module Settings 63
3.4.5 Changing Password Settings 65
3.5 Configuring Parent Link Settings 66
3.5.1 Parent Selection Method Settings 67
3.5.2 Client Parameters Settings 69
3.6 Configuring Advanced Network Settings 73
3.6.1 IGMP Settings 74
3.6.2 Other Network Protocols 75
3.6.3 Services 77
3.6.4 SNMP Agent 79
3.7 Configuring Quality of Service (QoS) Settings 80
3.8 Configuring VLAN Settings 82
3.9 Configuring NAT Settings 84
3.10 About The ELXM-SW6 86

4 Diagnostics and Troubleshooting 87

4.1 Checking the Ethernet Cable 87
4.2 LED Display 88
4.3 Resetting an ELXM-SW6 Radio to Factory Defaults 89
4.3.1 Resetting to Factory Defaults 89
4.3.2 Resetting to User Defaults 90
4.4 Unable to scan for AP's Error Message 91

5 Security 92

5.1 Scope 92
5.2 Defense in Depth 92
5.2.1 Defense in Depth vs. Hardening 93
5.2.2 Responsibilities 93
5.2.3 Example 93
5.3 Impact of the System Lifecycle to the Device Lifecycle 94
5.3.1 VLAN Plan 94
5.4 Impact of Device Requirements on System Planning 95
5.4.1 Secure Installation Location 95
5.4.2 Dedicated User Account Login Policy 96
5.4.3 Password Strength 96
5.4.4 Dedicated Logging Policy 96

6 Device Security 97

6.1 Prerequisites 97
6.2 Recommended Installation Sequence 97
6.2.1 Reasons for the Recommended Installation Sequence 97
6.2.2 Recommended Preparation for Installation 98
6.3 Choice of a Secure Installation Location 98
6.3.1 Device Availability Requirements 98
6.4 Software Update 99
6.5 Security Configuration 100
6.5.1 Disable Insecure Management Protocols 100
6.5.2 Create a Backup of Device-Specific Data 101
6.6 Possible Hardware Modifications for Security 101
6.6.1 Restrict Physical (Visual) Access to the Device and Port LEDs 101

6.7 Device Installation 102
6.8 Operation 102
6.8.1 Environmental Conditions 102
6.8.2 Connectivity 102
6.9 Maintenance 103
6.9.1 Software Update 103
6.9.2 Hardware Replacement 103
6.9.3 Hardware Repair 103
6.10 Decommissioning 104
6.10.1 Destruction of Confidential Data 104
6.10.2 Secure Physical Destruction of Device and Components 104

7 Initial Access - Cybersecurity 105

7.1 DHCPv4 Client 105
7.2 IH Browser 105

8 Appendix A - Radio Hardware 107

8.1 Radio Power Requirements 107
8.2 Ethernet Cable Specifications 108
8.3 Ethernet Cable Configuration 109
8.3.1 Ethernet Cable Configuration 109

9 Appendix B - ELXM-SW6 Virtual LAN (VLAN) Functionality 110

9.1 Transparent Support of VLAN Tags (802.1Q) 110
9.2 Port/Radio-based VLAN Tagging with Managed Switches 111
9.3 Port/Radio-based VLAN Tagging without Managed Switches 112

10 Appendix C - EtherNet/IP and Modbus TCP/IP Support 113

10.1 Modbus TCP/IP Server Support 113
10.1.1 Modbus Memory Map Diagnostic Information 113
10.2 EtherNet/IP™ Server Support 115
10.2.1 ELXM-SW6 Information 115
10.2.2 ELXM-SW6 Information Extended 116
10.2.3 File CRC Signatures 117

11 Appendix D - AP Channel-Frequency Table 118

12 Appendix E - Emission Regulations 120

12.1 2.4 GHz Band, FCC, Point-To-Multipoint 120
12.2 2.4 GHz Band, FCC, Point-To-Point 120
12.3 5 GHz Band, FCC, Point-To-Multipoint 121
12.4 5 GHz Band, FCC, Point-To-Point 121
12.5 6 GHz Band, FCC 121
12.6 2.4 GHz Band, ETSI 122
12.7 5 GHz Band, ETSI 122
12.8 6 GHz Band, ETSI 122

13 Appendix F - Detailed Radio Specifications 123

13.1 ELXM-SW6 Detailed Specifications 123
13.1.1 Radio....123
13.1.2 Physical....123
13.1.3 Environmental....124
13.1.4 Agency Approvals & Certifications....124

14 Glossary of Terms 125

15 Support, Service, and Warranty 130

15.1 Contacting Technical Support....130
15.2 Warranty Information 130

1 Start Here

1.1 Before You Begin

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

1.2 About This Manual

This manual covers the ProLinx Edge® 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

The ELXM-SW6 Radios can communicate with ProSoft Technology's RLX2 series of radios as well as third-party WiFi Access Points.

1.3 About ELXM-SW6 Industrial Hotspot Products

1.3.1 Product Overview

The ELXM-SW6 Radio 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 radio operates as a wireless Ethernet switch. Any data that can be sent over a wired network can also be sent over the radio.

The ELXM-SW6 is certified for unlicensed operation in the United States, Canada, Europe and other approved countries in the 2.4 GHz, 5 GHz and 6 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 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. All other legacy security protocols like TKIP and WEP are no longer supported.

The radio is designed for industrial client applications and can be either DIN-rail or panel mounted. Shock and vibration are tested to IEC 60068 2-27 and IEC 60068 2-6, respectively.

The ELXM-SW6 Radio series is easy to use. Access the built-in webpages with any web browser to configure the radio or use the Windows-based utility called *IH Browser*. It finds all the ProSoft 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.

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

You can download sample programs, utilities, firmware images, and documentation for your radio from the ProSoft Technology website (www.prosoft-technology.com).

1.3.2 General Features

The ProLinx Edge® 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 *Appendix F - Detailed Radio Specifications*. For descriptions of the LEDs, see section *4.2 LED Display*.



1.3.3 Antenna Port Connections

This section addresses physical antenna connections. Information regarding antenna selection and configuration can be found at www.prosoft-technology.com.

The ELXM-SW6 supports up to two antennas, configurable on the *Advanced Settings* page. For more information, see section *3.4.1 Advanced Wireless Settings*. Antennas must be connected to the radio when in use on the network.

Antenna port B is not available on this device but reserved for future use.

Mount all antennas that are directly connected to the radio so that polarization is the same. Screw the antenna onto the antenna port connector until snug.

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

External Antenna Requirements (EU / EN 303 687) for operation in the 6 GHz band:

The ELXM-SW6-E model for use in Europe, has a max output power of 14 dBm in the 6 GHz band. To be compliant with EU 6 GHz emission regulations, the antenna used with the ELXM-SW6-E must have a gain low enough to not exceed the limit using the following formula:

ELXM Max Tx Power + Max Antenna Gain <= Max PEIRP limit

where,

ELXM Max Tx Power = 14 +/- 2 dBm
Max Antenna Gain = The 6 GHz gain from antenna vendor's datasheet
Max EIRP Limit = 23 dBm, the 6 GHz CE EIRP Limit

Maximum Permissible 6 GHz Antenna Gain: 7.0 dBi (to maintain compliance with the 23 dBm EIRP limit for Low Power Indoor operation).

Be cautioned that each band has different power and EIRP limits, so that an antenna that meets the limits in one band might exceed the limits in another frequency band. See *Appendix E - Emission Regulations* for the FCC and EU CE limits.

Important: If the ELXM-SW6 is to be used in a hazardous location, mount the ELXM-SW6 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	

1.4 Package Contents

1.4.1 ELXM-SW6

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

Qty.	Part Name	Part Number	Part Description
1	ELXM-SW6 Radio	*Varies*	ProLinx Edge® ELXM-SW6 802.11ax Industrial Hotspot
1	Power Connector	350-1021	Mating power connector for the ELXM-SW6, for attachment to power supply.

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

1.5 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 Radios. It is designed for personal computers running the Microsoft Windows operating systems.

1.5.1 IH Browser System Requirements

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

- Microsoft Windows 10
- Microsoft Windows 11

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

1.5.2 Installing IH Browser Software

You must install IH Browser software to configure the radio as the ELXM-SW6 is not shipped with a default static IP Address.

To install IH Browser from the ProSoft Technology website

1. Open your web browser and navigate to www.prosoft-technology.com.
2. Use the search box on the ProSoft Technology page to search for *IH Browser* and then click the link for the *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 your *Windows Desktop*, so that you can find it easily when you have finished downloading.
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.

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

1.5.3 Starting the IH Browser

To start the *Industrial Hotspot Browser* (ID Browser), click **START > ALL PROGRAMS > PROSOFT > IH BROWSER**. For more information on the IH Browser and its functions, see section *2.4 Using the IH Browser to Configure* .

2 ELXM-SW6 Series Quick Setup

This chapter describes how to set up ELXM-SW6 Radios in a minimal configuration before deploying them in the permanent installation. The procedures in this section help familiarize you with basic configuration procedures and show you how to verify that the radios are operational.

The procedures described in this section assume the radios are in their default configurations as shipped by ProSoft. If that is not the case, you can reset the radios to factory defaults before attempting these procedures. For more information, see section *4.3 Resetting an ELXM-SW6 Radio 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 or a 3rd party vendor. Radios that you configure 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 allow you to confirm that the Client radios are configured correctly.

If you are replacing an existing radio with a new radio of the same type, you can easily transfer the radio configuration from the old radio to the replacement radio. For more information, see section *2.7 Replacing an Existing ELXM-SW6*.

2.1 Preparing the Configuration Environment

If you do not have an Access Point nearby to test the wireless connection or the Access Point is very close by (5 to 10 feet) you may not need antennas 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 radios, apply a label to each radio indicating the radio name and IP address.

2.2 Making Power and Data Connections

2.2.1 ELXM-SW6 Radio Connections

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



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

Ethernet Connection Speed	LINK LED
10 Base T	LED is off
100 Base T	LED blinks about twice a second
1000 Base T	LED is on

2.3 Power-Up

ELXM-SW6 Radios power up when power is supplied to the radio - there is no On/Off switch. The LEDs cycle when power is applied:

1) The Power LED turns on AMBER.
2) The Power LED turns on GREEN and the 1st Signal LED initially turns on AMBER.
3) The Signal LED then turns off and only the Power LED remains on and GREEN.
4) The activity LEDs start flickering, indicating the Radio is transmitting or receiving.
5) This process takes 10 to 15 seconds.

Please note the MAC address is printed on a label attached to the front of the Radio. The MAC address has the form **00-0D-8D-F4-YY-ZZ**. This number uniquely identifies the Radio on the network. Use this number to identify the Radio on the network when using the IH Browser.

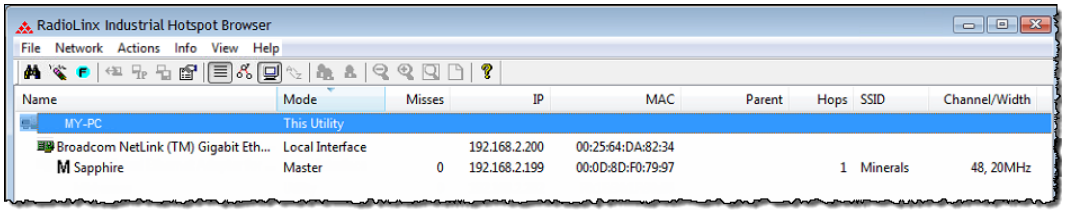
2.4 Using the IH Browser to Configure the ELXM-SW6

This section describes how to use the IH Browser to set up an ELXM-SW6 in a minimal configuration before deploying it in a permanent installation. See section *2.4 Using the IH Browser to Configure* for detailed descriptions of all the features available in the IH Browser.

2.4.1 Viewing the Radios in the IH Browser

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

The *List* view (shown in the image below) displays the ELXM-SW6 (or previous generation RLX2) 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: You can perform many common tasks by right-clicking on the radio and choosing a command.

2.4.2 Refreshing the Display in the IH Browser

To refresh the display

If you have made changes 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 Radios (or from the *File* menu choose **SCAN**).

2.4.3 Setting the Radio IP Address in the IH Browser

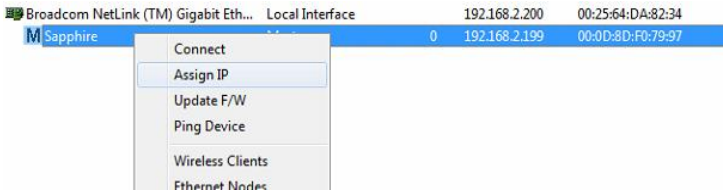
To set the radio IP address

- If the ELXM-SW6 is 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**. You can assign a temporary IP address to assist with configuring the ELXM-SW6. For more information, see section *2.4.4 Assigning a Temporary IP Address*.

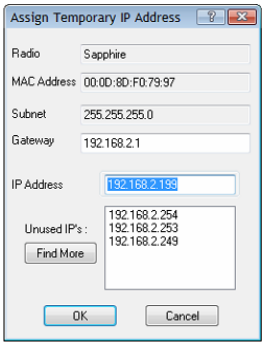
2.4.4 Assigning a Temporary IP Address

A temporary IP address allows you to access and configure an ELXM-SW6 when it either does not have an IP Address, or it has an IP Address 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**.

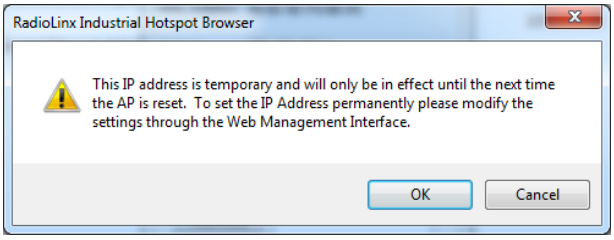


This opens the *Assign Temporary IP Address* dialog box.



The *Unused IP's* list are the IP addresses that are currently 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. Your radio should now appear in the IH Browser window with the temporary IP address.

4 To set a permanent IP address for the radio, see section *2.5 Configuring an ELXM-SW6 - Getting Started*.

2.5 Configuring an ELXM-SW6 - Getting Started

This section describes how to set up ELXM-SW6 Radios in a minimal configuration before deploying them in the permanent installation. See section *3.3 Configuring Basic Settings* for detailed descriptions of all the configuration parameters.

2.5.1 Connecting to the Radio Configuration Interface

This section describes how to connect to the ELXM-SW6 web interface using a web browser such as Internet Explorer or Firefox on your PC or other network-enabled device.

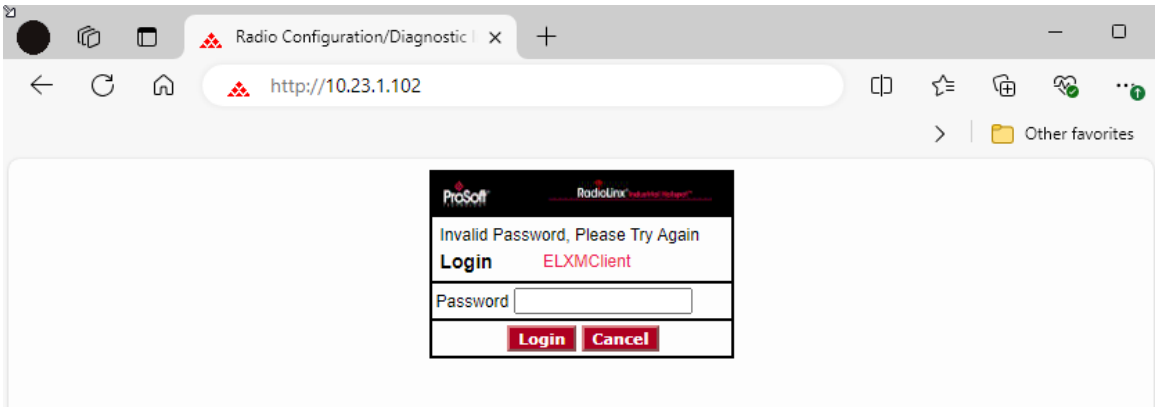
To connect to the Radio Configuration / Diagnostic web interface

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

1 Log into the web interface of the radio. You can do this in any of three ways:

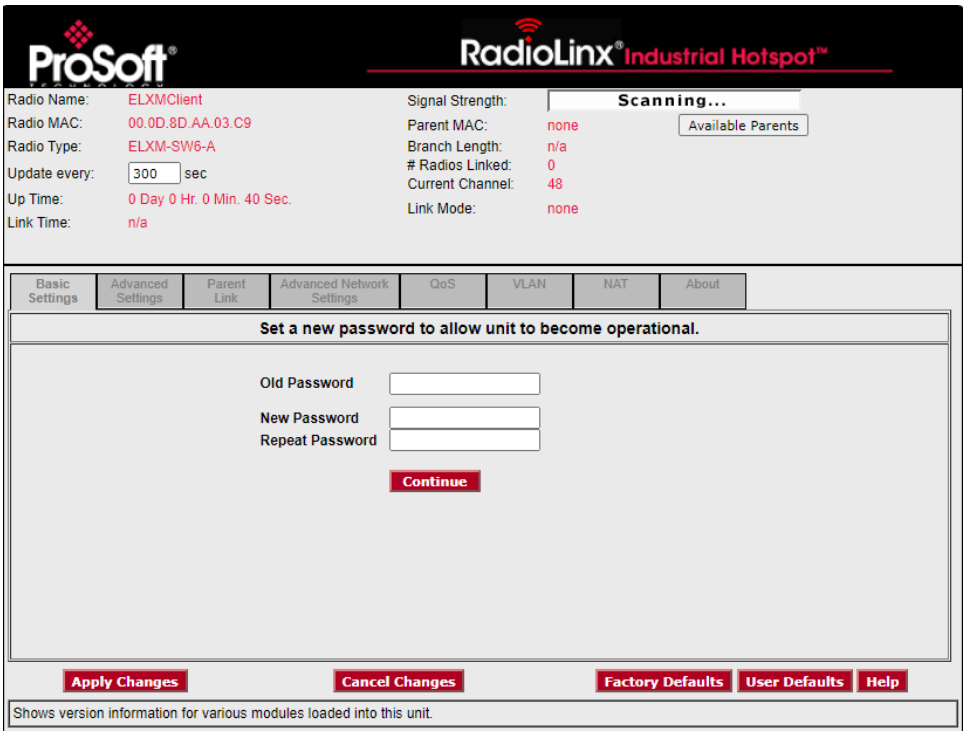
- In the IH Browser List view or Topography view, right-click the radio and then click **CONNECT**.
- In the IH Browser List view or Topography view, double-click the radio.
- Open a web browser on your PC, and then in the address bar, type `http://` followed by the IP address for the radio, and then press **ENTER**.
  For example: `http://10.23.1.102`

The login screen appears in the web browser.

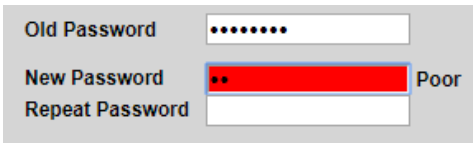


2 Enter the password and then click **LOGIN**. The default password is *password*. If you have lost the password for the radio, you can reset the radio to its default settings. For more information, see section *4.3 Resetting an ELXM-SW6 Radio to Factory Defaults*.

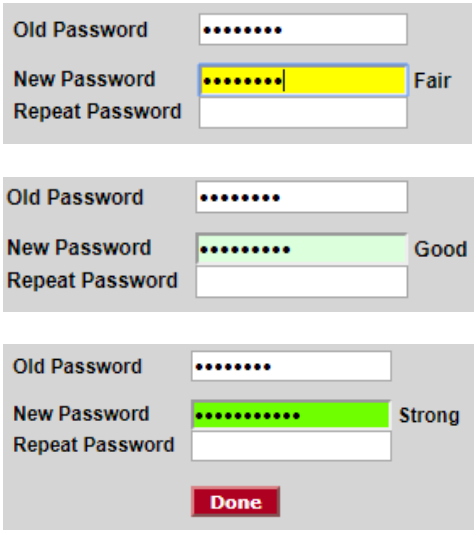
3 If the radio is set to its factory settings or has been reset to defaults, then the first page that opens requires a new password to be set before the configuration tabs are enabled. This is to ensure that the radio is not unintentionally put into operation using the factory default password.



4 Type the default password into the *Old Password* edit box, then a password with sufficient security strength into the *New Password* edit box.



5 As you type in the new password the security strength is indicated to the right of the edit box and in its background color.



6 The password entered is measured against 4 categories. Each of the categories must be satisfied to achieve a “strong” password strength.

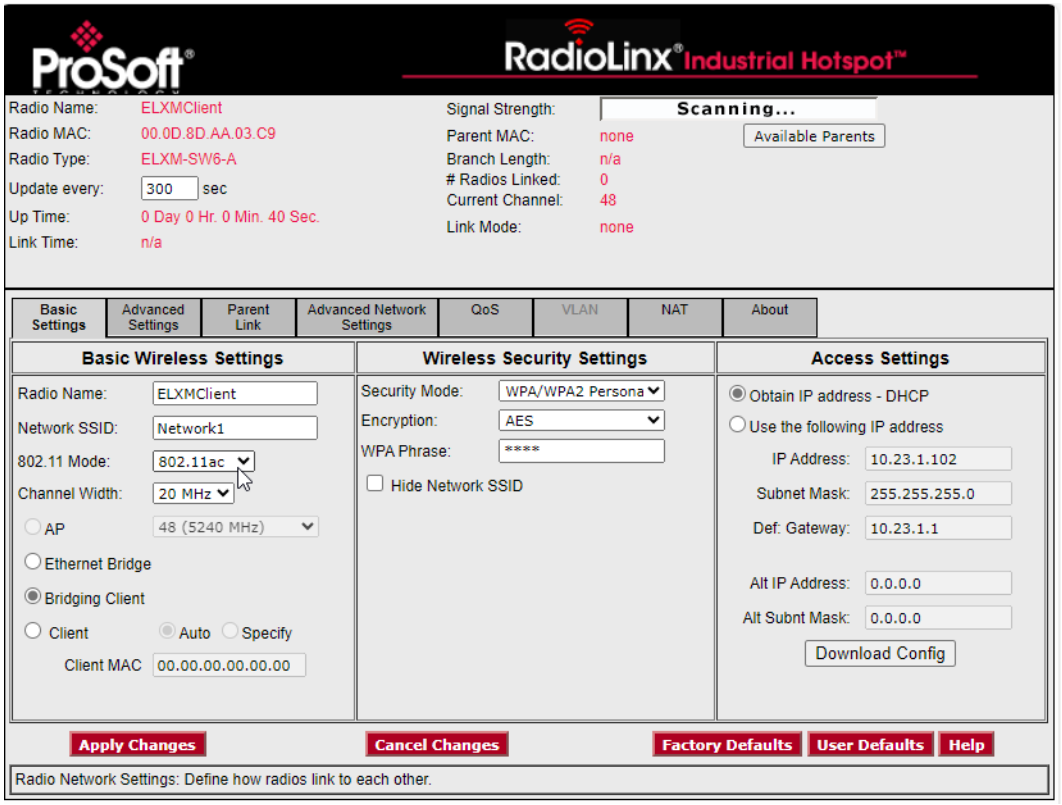
- Must contain both lower- and upper-case letters
- Must contain one or more numbers
- Must contain at least one non-alphanumeric character (e.g. !@#$).
- Must be at least 8 characters in length.

In addition, if the default password is embedded in the New Password, then those characters are ignored when testing for each of the above criteria.

7 After entering the New Password, the password is entered once again in the **REPEAT PASSWORD** edit box to mitigate any typing errors.

8 Clicking the **CONTINUE** button opens the main configuration webpage of the radio.

Note: Some parameters may be different from the image depending on your specific radio model.



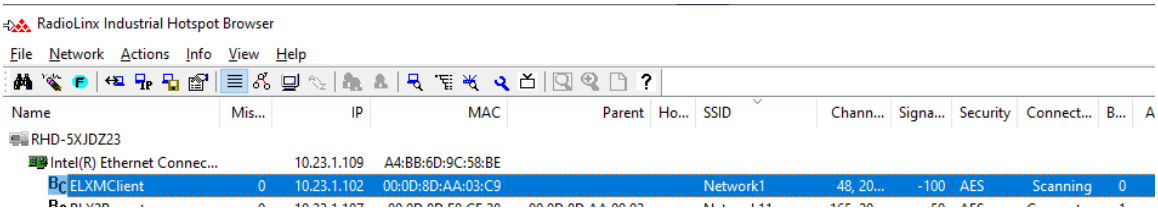
Tip: You can display the help topic for any parameter in the ELXM-SW6 webpage by clicking the parameter name. The parameter name turns blue when you move the cursor over a parameter with a help topic. There is also a short description at the bottom of the window.

2.5.2 Configuring a Bridging Radio

If the wireless network will be using **ProSoft RLX2** radios as the Access Points, the ELXM-SW6 should be configured in Ethernet Bridging mode.

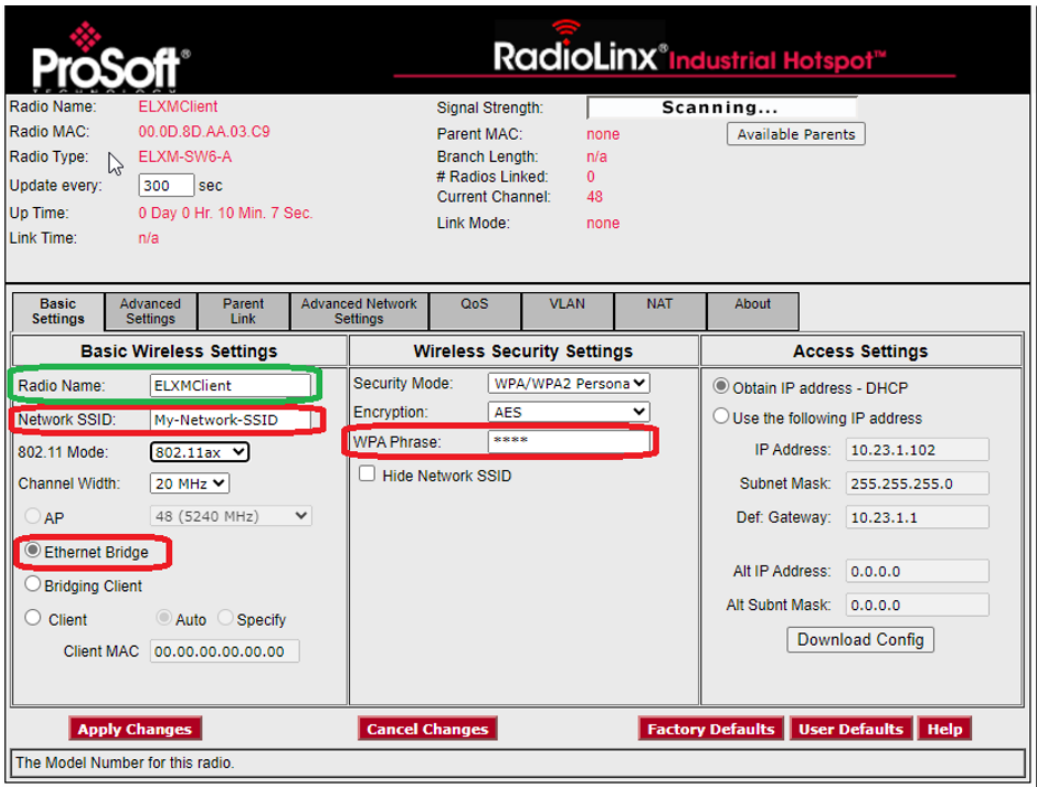
To configure an Ethernet Bridging radio

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

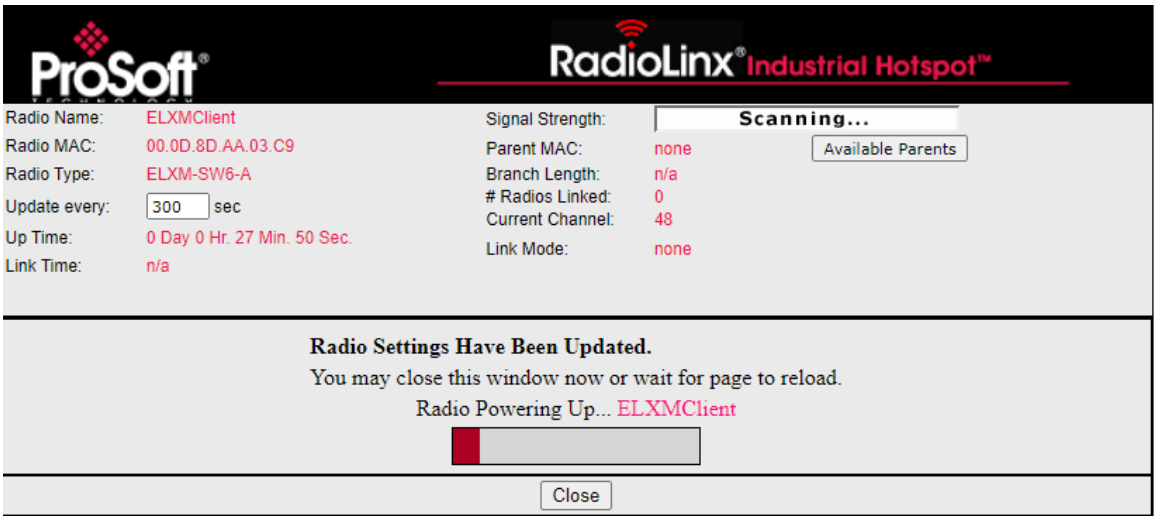


2 If the radio IP address is **0.0.0.0**, assign a temporary IP address to the ELXM-SW6 Radio. For more information, see section *2.4.4 Assigning a Temporary IP Address*. In this example, the ELXM-SW6 has an IP address of **10.23.1.102**.

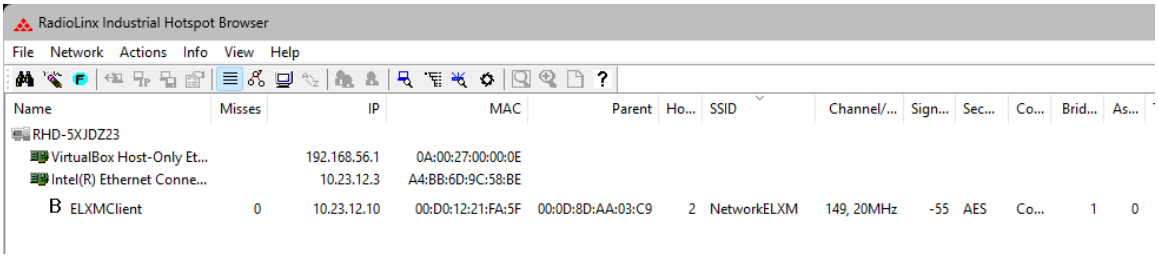
3 Log into the radio's web interface. For more information, see section *3.1 Connecting to the Radio Configuration Interface*.



4 The fields highlighted in red above must be set as a minimum for the ELXM-SW6 to connect to a ProSoft access point.
5 On the *Basic Settings* tab, in the *Basic Wireless Settings* group, change the radio to **ETHERNET BRIDGE** and set the *Network SSID* and *WPA Phrase* to match that of the Access Points with the same SSID.
6 Although not strictly necessary, set the *Radio Name* to something unique in your system (e.g. **ELXMClient** as shown above) either with a number or where the radio will be used.
7 Click **APPLY CHANGES** to reboot the Radio.



8 After successfully rebooting, the radio appears as an Ethernet Bridge radio in the IH Browser window:

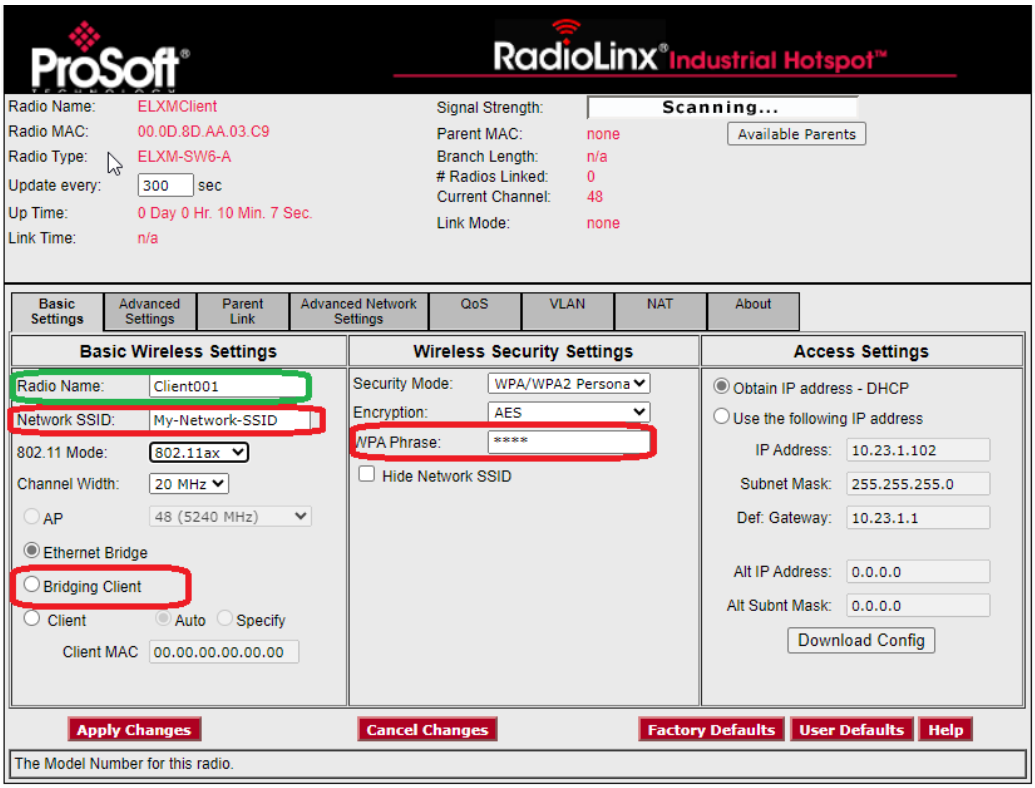


2.5.3 Configuring a Bridging Client Radio

You can configure ELXM-SW6 Radios in *Client* or *Bridging Client* modes if you want to connect to third-party 802.11 Access Points. See section *2.5.4 Configuring 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.

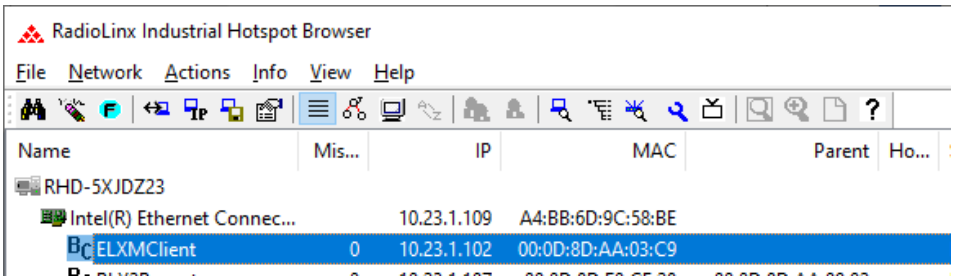
To configure a Bridging Client radio

1. Power up a new radio in the default configuration.
2. Start the IH Browser. After the radio starts, it should appear in the IH Browser.
3. In the IH Browser, assign a temporary IP address to the Repeater radio. For more information, see section *2.4.4 Assigning a Temporary IP Address*.
4. Log into the radio. For more information, see section *3.1 Connecting to the Radio Configuration Interface*.
5. On the *Basic Settings* tab, in the *Basic Wireless Settings* group, change the radio to **BRIDGING CLIENT** and set the *Radio Name, Network SSID,* and *WPA Phrase* accordingly.



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

7 Refresh the display in the IH Browser. The radio 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 a Client Radio

The ELXM-SW6 can be configured in *Client* mode if you want to connect to third-party 802.11 Access Points, and your application is using non-IP based protocols. The following table highlights the most significant differences between Bridging, Client, and Bridging Client modes on the ELXM-SW6.

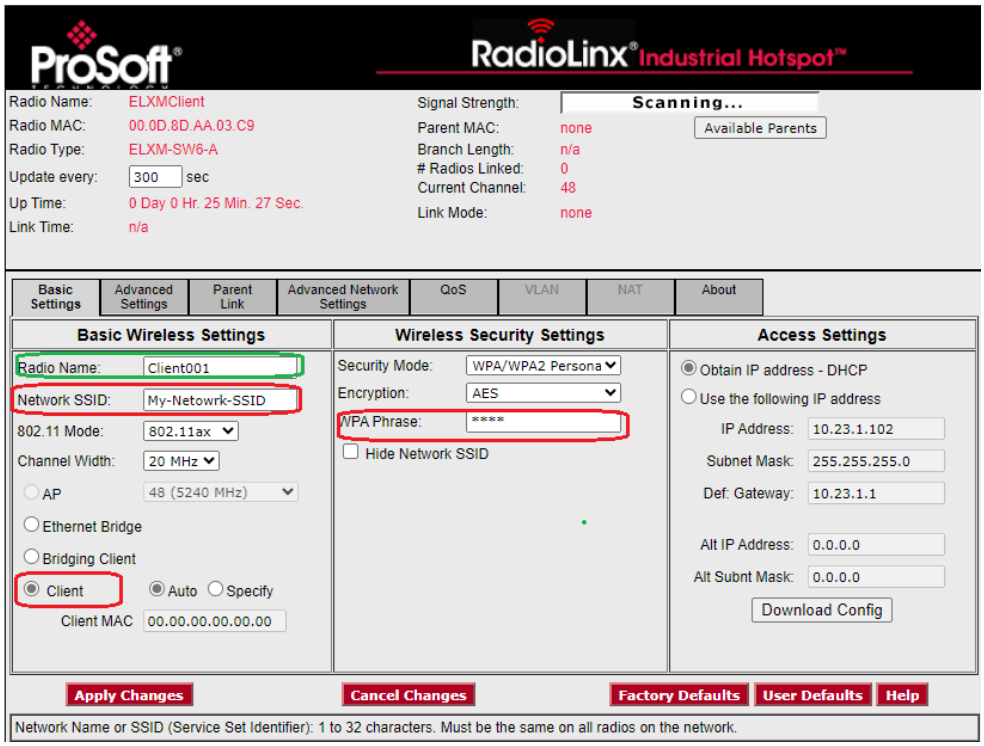
	Bridging	**Client**	**Bridging Client**
Number of attached Ethernet devices supported	Multiple (up to the limits of network)	One	Multiple (up to 16)
Can other wireless devices connect to the radio?	No	No	No
Can the radio connect to non-ProSoft Technology Access Points	No	Yes	Yes
MAC Addresses seen on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

Client mode is a special mode 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 with an RJ45 Ethernet port can, in effect, become an 802.11 wireless client by attaching the radio. 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).

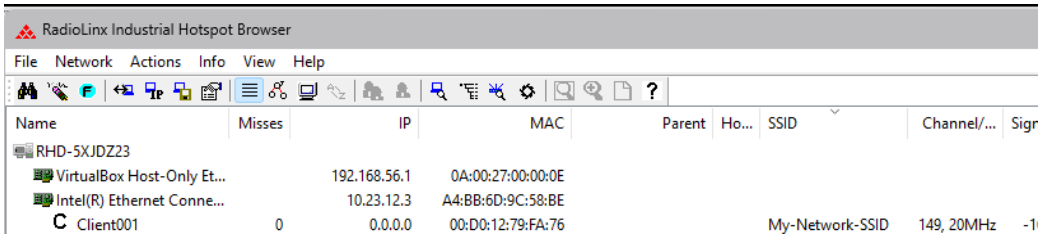
Note: Use Client mode if you need to connect to another brand access point **and** your application is using non-IP based protocols. If you are using ProSoft Radios as Access Points, use the ELXM-SW6 in Bridging mode which transparently transports all Ethernet frames at the MAC level (layer 2 bridging). If you do not need a Client ELXM-SW6 Radio in the system, you can skip this example configuration.

To configure a Client radio

1 Power up a new radio and configure it to connect to an access point.
2 Start the IH Browser. After the radio starts, it should appear in the IH Browser.
3 In the IH Browser, assign a temporary IP address to the Repeater radio. For more information, see section *2.4.4 Assigning a Temporary IP Address*.
4 Log into the radio. For more information, see section *3.1 Connecting to the Radio Configuration Interface*.
5 In the *Basic Wireless Settings* group, change the radio to **CLIENT**.



6 Edit the *Radio Name* if desired.
7 Set the *Network SSID* and *WPA Phrase* to match that of the wireless network.
8 If you set a temporary IP address in the radio (For more information, see section *2.4.4 Assigning a Temporary IP Address*), set the permanent IP address in the *Access Settings* group. Click **OBTAIN IP ADDRESS - DHCP** or **USE THE FOLLOWING IP ADDRESS**.
9 Click **APPLY CHANGES** to reboot the Radio.
10 Refresh the display in the IH Browser. The radio appears in the IH Browser as a Client radio.



11 When the Client radio reboots, wait until the radio registers the MAC address of the PC's Ethernet interface (Client mode only).
12 Ensure that the IP address of PC is on the same subnet as the AP network for the SSID. For this example, set the IP address of the PC interface to **192.168.2.248**.
13 Open a command prompt on the PC and verify that you can use the Ping command to ping the IP address of the Master radio.

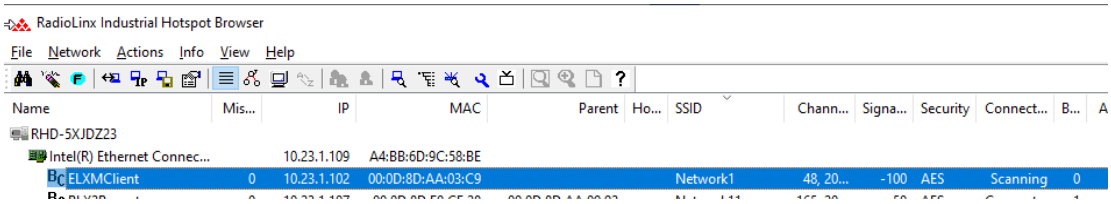
2.5.5 Configuring as Soft Access Point (Soft AP)

The ELXM-SW6 can operate as a simple Access Point, typically called a "SoftAP". It provides the same functionality as the RLX2-IHx in AP mode with the following limitations:

- The ELXM-SW6 AP can only operate on the 2.4 GHz and 5 GHz bands. The 6 GHz band operation is not supported.
- The DFS channels in the 5 GHz band are omitted.
- The number of simultaneously connected client devices is limited to 12.
- The IGMP feature is permanently disabled.
- WPA3 Security modes are disabled.

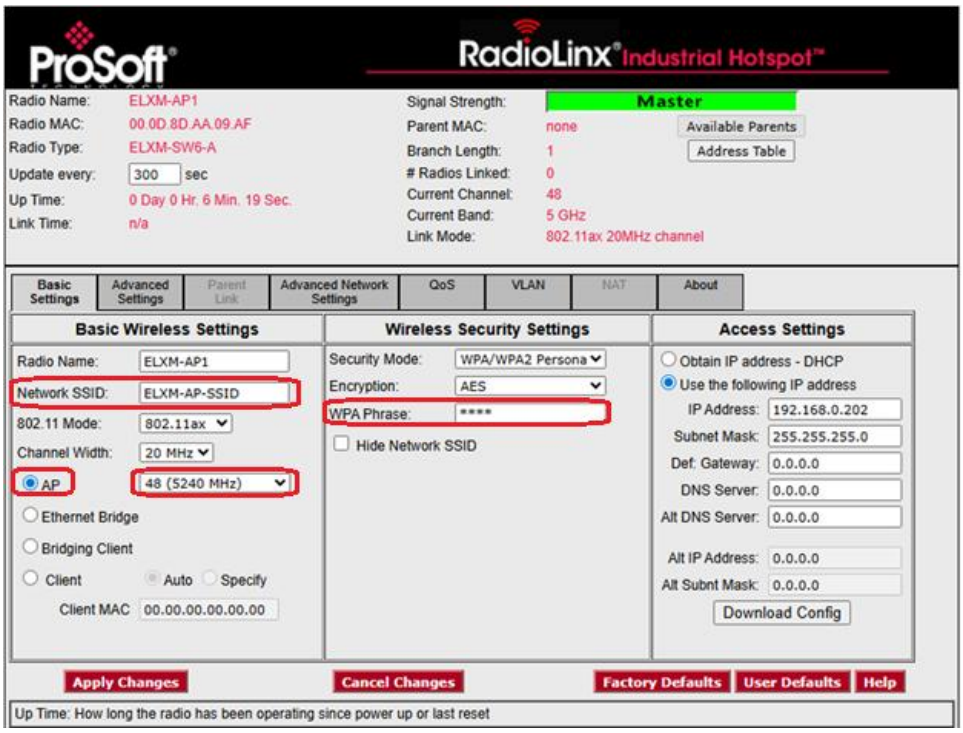
2.5.5.1 To configure an AP radio

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



2 If the radio IP address is **0.0.0.0**, assign a temporary IP address to the ELXM-SW6 Radio. 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 radio's web interface. For more information, see section *3.1 Connecting to the Radio Configuration Interface*.

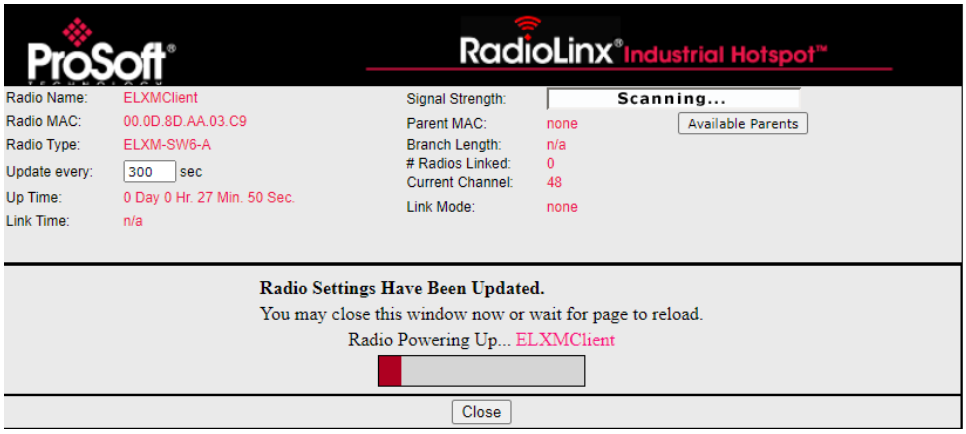


4 The fields highlighted in red above must be set as a minimum for the ELXM-SW6 to operate as an access point.

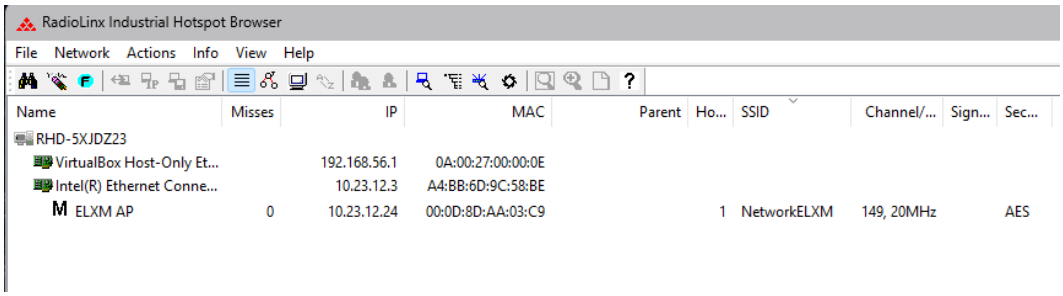
5 On the *Basic Settings* tab, in the *Basic Wireless Settings* group, change the radio to **AP** and set the *Network SSID* and *WPA Phrase* to match the wireless settings required by the Network administrator.

6 Although not strictly necessary, you should set the *Radio Name* to something unique in your system (e.g. **ELXM-AP1** as shown above) either with a number or where the radio will be used.

7 Click **APPLY CHANGES** to reboot the Radio.



8 After successfully rebooting, the radio appears as an AP radio in the IH Browser window. The symbol **M** is used by the RLX2-IHx AP denoting the radio is a "Master" as opposed to a client.



2.6 Viewing an ELXM-SW6 Configuration

You can quickly view a radio's configuration.

1. Start the IH Browser.
2. Right-click the radio and then click **PROPERTIES**.
3. If you want to view all the available properties, in the *Detailed Information for Radio* dialog box, click **MORE**. Note that you cannot change the radio's configuration in this dialog box.

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 the optional microSD card in the back of the radio.

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

If you are replacing an existing radio that has a Personality Module (microSD card) installed, then you do not need to manually configure the new radio. Remove the microSD card from the existing radio with the stored configuration and install it in the new radio. When you power up the new ELXM-SW6 Radio, the new radio uses all the configuration settings from the microSD card. This feature eliminates the need to manually configure the replacement radio.

If a microSD card is used, by default the ELXM-SW6 Radios writes configuration changes to the microSD card whenever you make configuration changes. The ELXM-SW6 by default also reads the microSD card's configuration when it powers on and uses the stored configuration from the microSD card.

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

The file is encrypted on the microSD card so the configuration information (principally the configuration password and encryption key) cannot be extracted. We highly recommend that you physically secure the radio and the microSD card.

If you are not using the Personality Module (microSD card) feature, we recommend that you uncheck the **SD AUTO CLONE ENABLE** and **SD AUTO WRITE ENABLE** features. For more information, see section *3.4.4 Personality Module Settings*.

3 Configuring a Radio - Detailed Configuration

The ELXM-SW6 includes a built-in webserver that allows you to both monitor and to configure your radio. The webpages can be displayed from any computer that can connect to the radio through a wired Ethernet connection or a wireless connection.

You can monitor and change the settings for your radio using a web browser such as Microsoft Edge, Firefox, or Chrome. It can be accessed by using desktop PCs, laptops, tablets, or smart phones.

3.1 Connecting to the Radio Configuration Interface

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

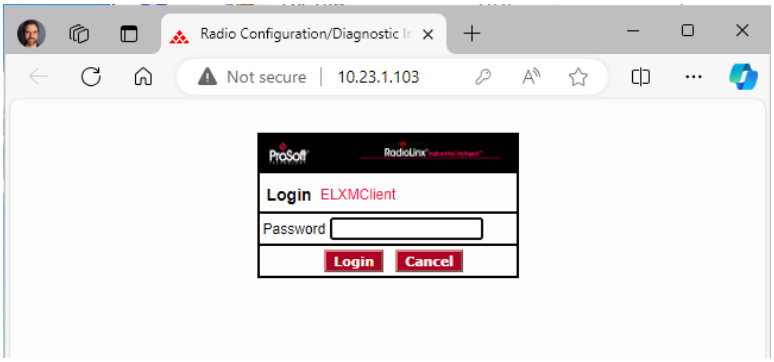
To connect to the radio

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

1 Log into the radio. You can do this in any of three ways:

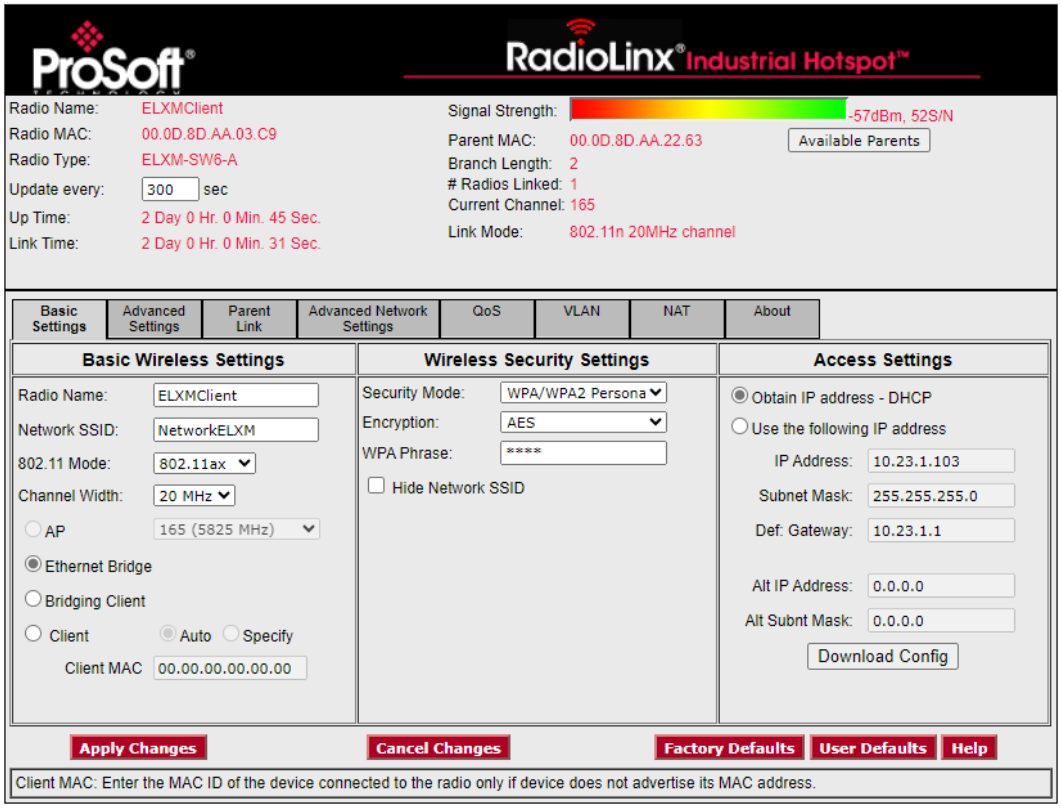
- In the IH Browser List view or Topography view, right-click the radio and then click **CONNECT**.
- In the IH Browser List view or Topography view, double-click the radio.
- Open a web browser on your PC, and then in the address bar, type `http://`, followed by the IP address for the radio, and then press **ENTER**. For example, `http://10.23.1.103`

The login screen appears in the web browser.



2 Enter the password and then click **LOGIN**. The default password is *password*.
If the radio is set to factory default, see section *2.5.1 Connecting to the Radio Configuration Interface* for entering an initial password to enable the configuration tabs.
If you have lost the password for the radio, you can reset the radio to its default settings. For more information, see section *4.3 Resetting an ELXM-SW6 Radio to Factory Defaults*.

3 This opens the main configuration webpage for the radio. Note that some parameters may be different from the image depending on your specific radio model.



Tip: You can 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.

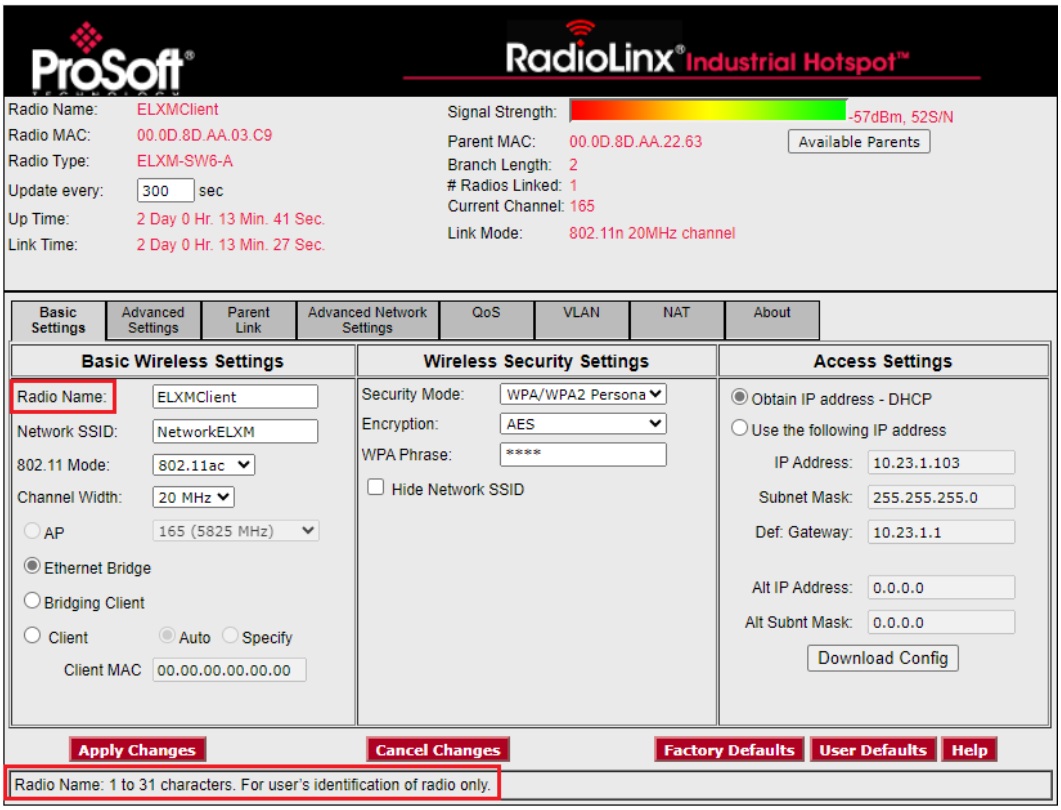
3.1.1 Read-Only Fields

Some of the parameters are for display and only provide information about the current state of the radio.

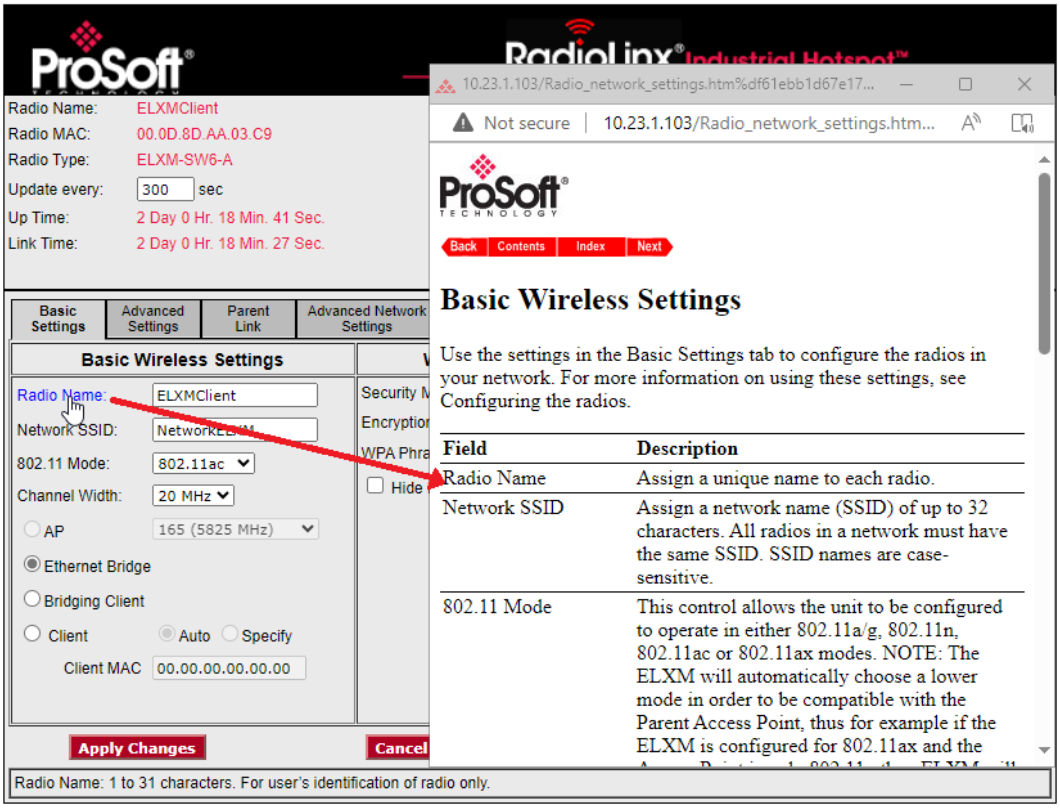
Note that depending on the model of the radio, and the radio configuration, some parameters and buttons may not be available or appear on the page.

3.1.2 Configuration Help

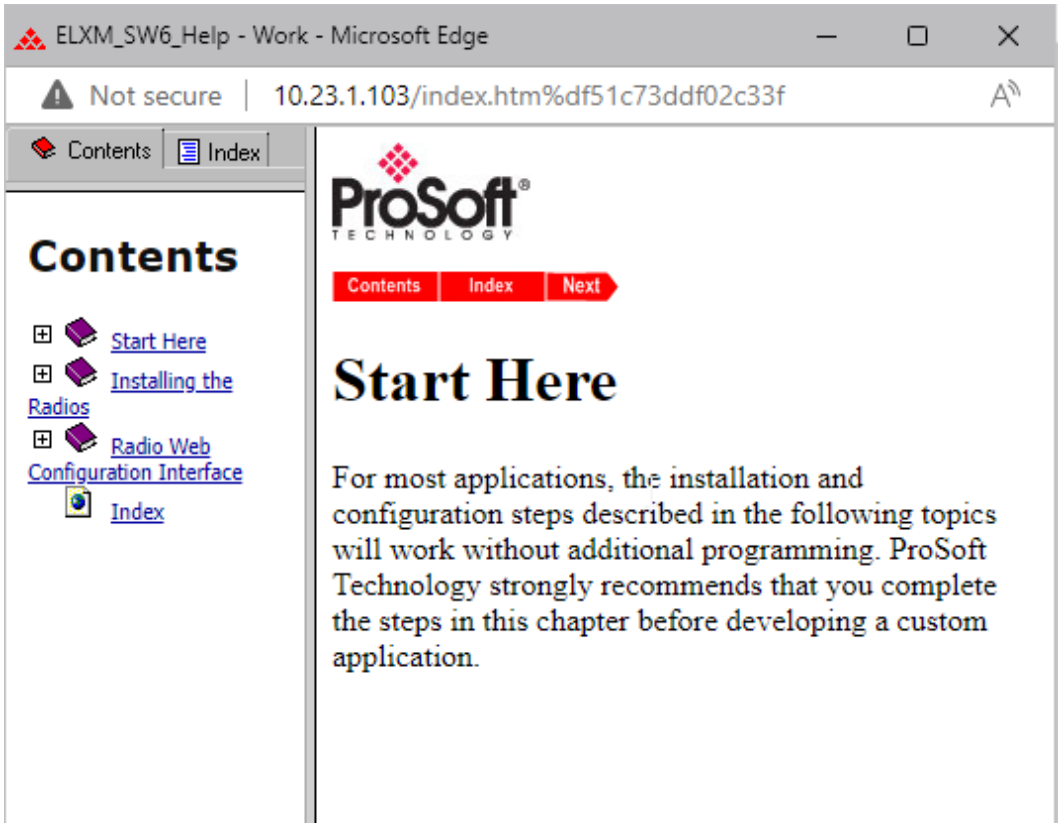
Help is available for each item on the webpage. To view a brief help message about any parameter on the screen, move the cursor over the parameter until the parameter name turns blue, or press the **TAB** key to select the parameter. Refer to the text that appears at the bottom of the screen.



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

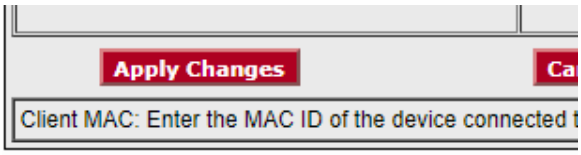


To view the complete online documentation for the ELXM-SW6 Radio, click the Help button. This action opens the online documentation in a new browser window. Use the **Contents**, **Index** and **Search** tabs in the left frame to navigate the help system.

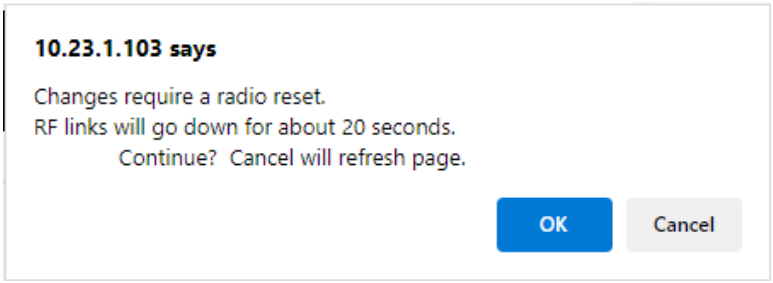


3.1.3 Apply Changes

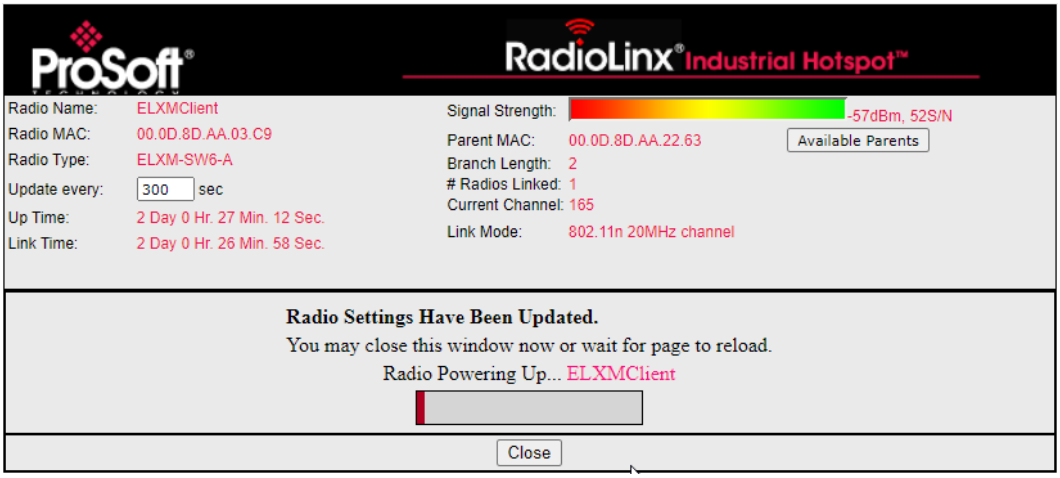
Click **APPLY CHANGES** to save changes to the radio configuration and restart the radio with the new configuration.



A pop-up dialog appears indicating that a reset is required and asks for confirmation to proceed.

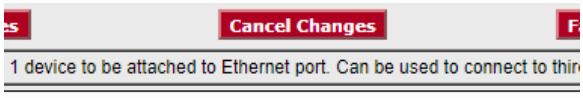


A progress bar appears after you click **OK**.



3.1.4 Cancelling Changes

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



A similar action can be achieved by refreshing the webpage.

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

3.1.5 Factory Defaults

Click **FACTORY DEFAULTS** to reset the radio to the original factory default settings.



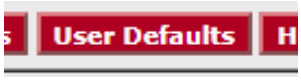
Important: This action discards all changes you have made to the radio configuration settings.

Two things to note if there is a microSD card in the radio's Personality Module slot.

- Clicking **FACTORY DEFAULTS** does not reset the configurations stored on the microSD card in the radio's Personality Module slot.
- If you select **SD AUTOWRITE ENABLE** on the *Advanced Settings* tab, the radio overwrites the configuration on the microSD card with the factory default settings if you click **APPLY CHANGES**. For more information, see section *3.4.4 Personality Module Settings*.

3.1.6 User Defaults

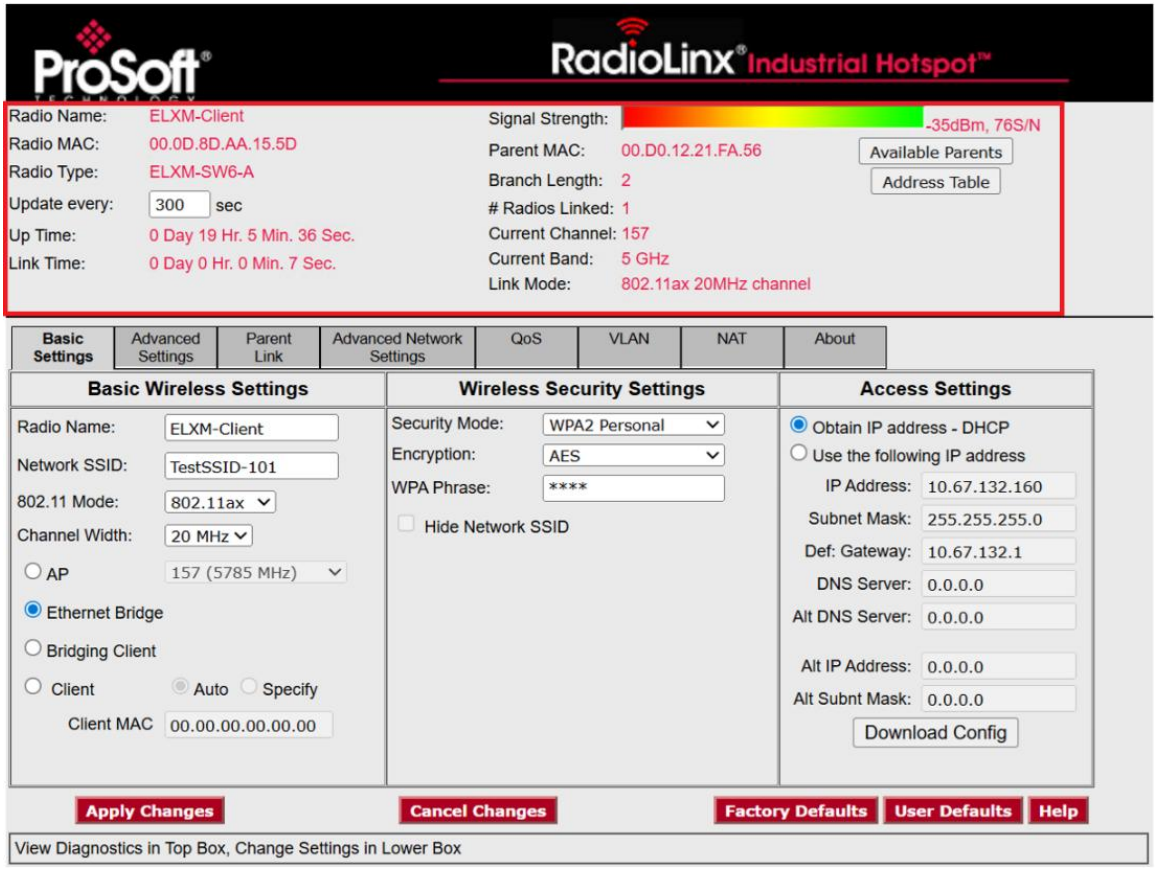
Click **USER DEFAULTS** to reset the radio to the last user defaults configuration file that was uploaded into the ELXM-SW6.



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

3.2 Viewing Radio Status

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



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

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

Parameter	Description
Radio Name	The user-assigned name for the radio.
Radio MAC	The MAC address of the selected radio. The MAC ID is also printed on the side of the radio.
Radio Type	The Model Number of this radio; for example: *ELXM-SW6-A*
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 radio has operated since the last system power-up or reset.
Link Time	The length of time that the radio has been continuously connected to the parent.
Signal Strength	The strength of the signal from the parent in absolute dBm and relative S/N (Signal to Noise) values.
Parent MAC	The MAC address of the parent to which the radio is linked.
Branch Length	The number of RF links from the radio to the Master radio.
# Radios Linked	The number of other radios that are linked to this radio.
Current Channel	The current operating channel for the radio. 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 radio is in 40 MHz mode, this parameter shows the main channel number, followed by the extension channel's number.
Current Band	The current operating Frequency Band: 2.4 GHz, 5 GHz or 6 GHz.
Link Mode	The 802.11 Mode in which the radio 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 this radio can detect beacons. This button is only available when the radio is in a Client mode (set in the *Basic Wireless Settings*). For more information, see section *3.2.1 Viewing Available Parents for a Radio*.

3.2.1 Viewing Available Parents for a Radio

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

Available Access Points ELXM-Client Only Show Same SSID: ☐ **Refresh**

00.0D.8D.AA.15.5D TestSSID-101 ELXM-Client *Click on column header to sort*

MAC ID	SSID	Channel	RSSI	Security	Encrypt	Speed	Cost	Age(s)	Hops
00:0d:8d:f0:96:f9	TestSSID	157	-75	WPA2.Prsl	AES	n	286	0	1
00:0d:8d:f0:97:1a	----------	157	-64	WPA2.Prsl	AES	n	200	2	2
00:0d:8d:f0:cb:c1	TestSSID	157	-82	WPA2.Prsl	AES	n	394	1	1
00:d0:12:21:fa:56	TestSSID-101	157	-35	WPA2.Prsl	AES	ax	38	0	1
44:c3:06:70:00:97	ELXM	157	-86	WPA2.Prsl	AES	ax	469	1	na

This page is helpful for viewing:

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

Note: You can click on a column header to sort the table by the values in that column

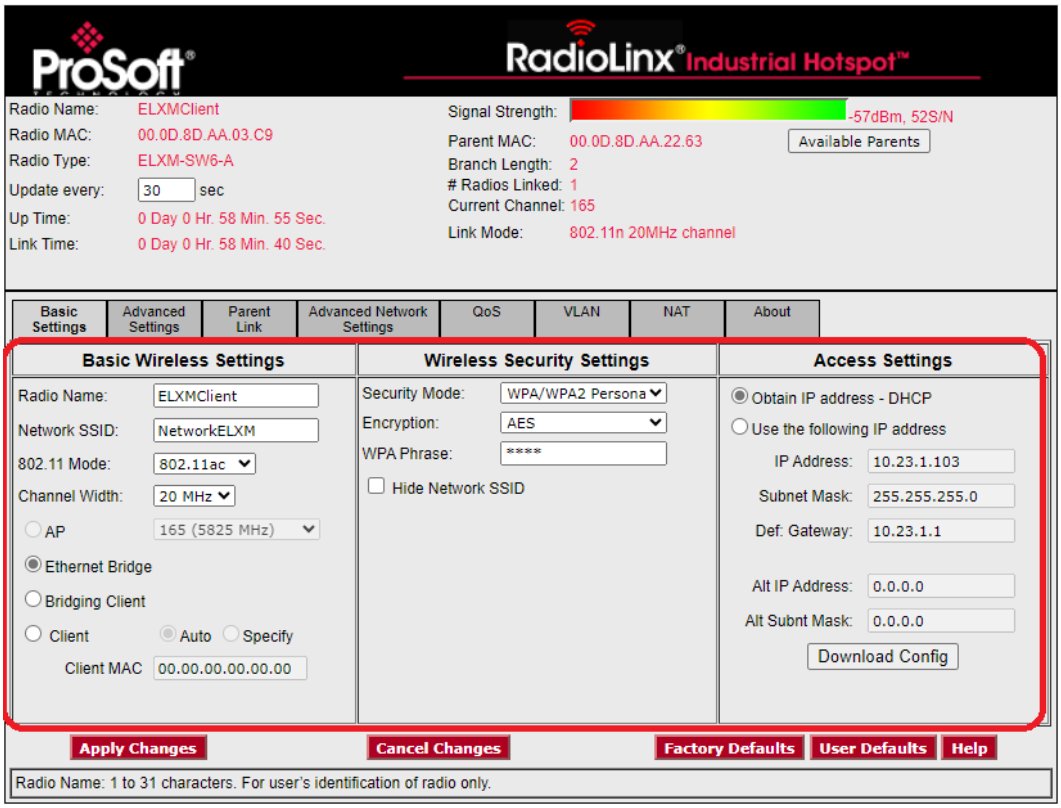
Parameter	Description
Only Show Same SSID	Select this check box to restrict the list of available parents to those with the same SSID as the radio you are configuring.
Refresh	Click this button to re-scan the network and update the devices in the list.
Mac ID	Displays the unique hexadecimal MAC Address 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 transmitted. If the *Speed* value is not **ax6g**, the band (2.4 GHz or 5 GHz) can be derived from the channel number. Channel < 15 = 2.4 GHz Channel > 15 = 5 GHz If the *Speed* value is **ax6g**, then the channel number is a 6 GHz channel. **Note:** The 6 GHz band re-uses the *Channel* value space resulting in a 6 GHz channel number being the same as one in the 2.4 GHz or 5 GHz band. **Available Access Points** ELXM-EW6-ArubaClient Only Show Same SSID: ☑ **Refresh** 00.0D.8D.AA.17.5A AP734-SCLAB-1X ELXM-EW6-ArubaClient *Click on column header to sort* MAC ID / SSID / Channel / RSSI / Security / Encrypt / Speed / Cost / Age(s) / Hops 48:00:20:14:58:94 / AP734-SCLAB-1X / 133 / -54 / WPA2&3.Ent / AES / ax6g / 79 / 0 / na
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, ax or ax6g). The ELXM-SW6 Radio supports all these 802.11 connection speeds.
Cost	Displays the calculated parent selection cost. The radio evaluates the link to its parent once per second to determine if this link is the best parent to use. The radio calculates the cost for each entry. The cost calculation is based not only on the strongest signal, but on other factors to provide optimum network communication.
Age(s)	Displays the length of time (in seconds) since the radio 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 continuously updated.
- The radio 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

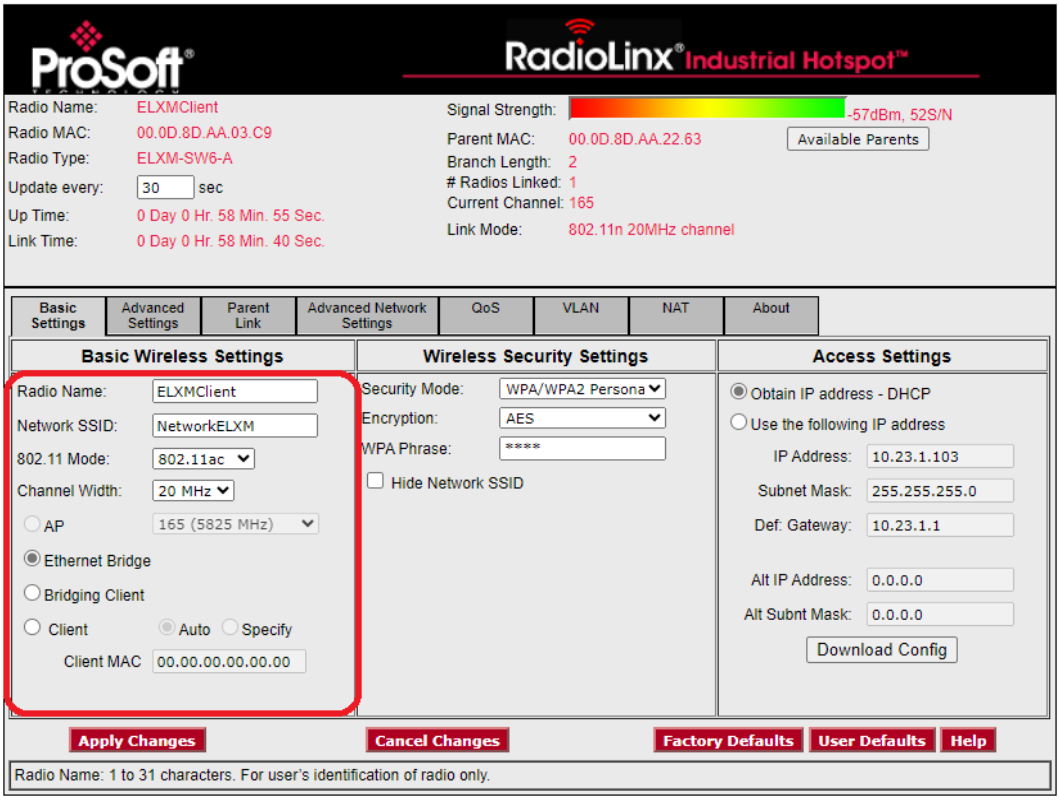
The **BASIC SETTINGS** tab includes three groups:

- 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 Radio.



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

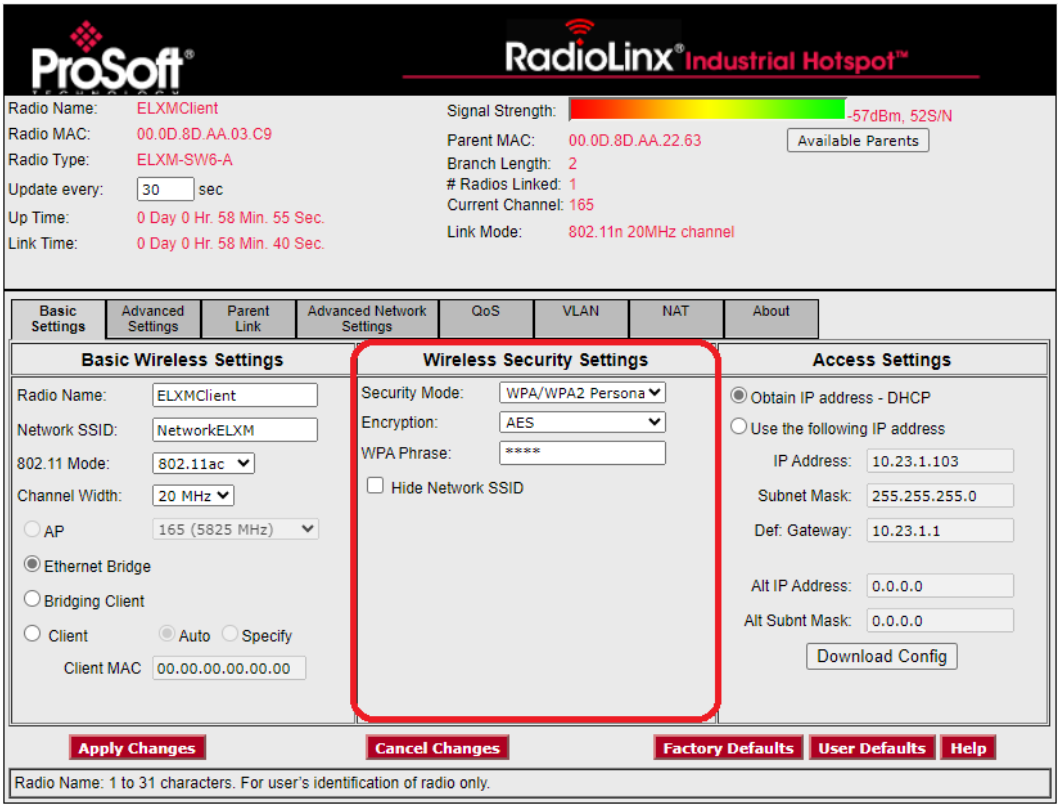
Parameter	Description
Radio Name	Specifies a unique name for the radio you are configuring.
Network SSID	Specifies a network name (SSID) of up to 32 characters and defines the network that this radio will join and be part of. All radios with this SSID are part of the same network. **Note:** SSID names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

Parameter	Description
802.11 Mode	Specifies the version of the 802.11 standard that will be used by the radio. **Note:** A radio 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 radio 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 the 802.11n/ac/ax operational features are disabled. It is **not** necessary to select this mode for ELXM-SW6 Radios to link to APs that only support 802.11a/g. The ELXM-SW6 will revert to the mode of the peer (AP or Client) if its mode is lower than this setting. If the peer mode is higher than this setting, then the ELXM-SW6 will force operation mode to this setting. This mode is not commonly used. It is mainly used to force operation at 802.11a/g rates if needed due to environmental or compatibility issues. The 802.11a/g mode only supports 20 MHz channels. **802.11N -** All 802.11n features are operational, and the radio 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 radio uses 20 MHz, 40 MHz or 80 MHz wide channels. **802.11AX -** All 802.11ax features are operational, and the radio uses 20 MHz, 40 MHz or 80 MHz wide channels.
Channel Width	Specifies the width of the channel that the radio will use when transmitting. When in Client Mode: Control options include 20 MHz and Auto. 20 MHz setting forces operation with peer using 20 MHz regardless of width supported by the AP. Auto setting will use the highest channel width supported by the AP. When in AP Mode: Control options include 20 MHz and 40 MHz widths. The 80 MHz option is not supported. **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 Radios will only transmit at this channel width if it is supported by a peer radio. Channels in the 5 GHz and 6 GHz bands are 20 MHz apart, so the 40 MHz channel width occupies only two channels in that band. However, channels in the 2.4 GHz band are spaced five MHz apart, so 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 Radios 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, 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	Specifies that this radio will operate as an 802.11 AP. The AP is the root device in a network. You must have at least one AP in your network. For redundancy, you can assign more than one AP to a network.
AP Channel (For AP mode only)	Specifies the channel number to be used by the AP. The channels are sorted by frequency band (2.4 GHz, 5 GHz), and the channel frequency in MHz. **Note:** DFS channels are omitted when in AP mode. **For ELXM-SW6 Radios:** In AP mode, when you set **CHANNEL WIDTH** 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 Radio is not supplied with an antenna. When choosing an antenna for use with your ELXM-SW6 Radio, you must choose one that supports the frequency range set in the configuration for the radio.
Ethernet Bridge	Specifies this radio is a Client radio that can only be used when all radios in the network (SSID) are ProSoft radios. In this mode all data packets are bridged at layer 2 between the ELXM-SW6 client and the ProSoft 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 this radio. For more information, see section *2.5.3 Configuring a Bridging Client Radio*.
Client	This mode allows you to transparently connect a single Ethernet device to any non-ProSoft 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 information, see section *2.5.4 Configuring 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 this radio, 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 of the ELXM-SW6 Radio.



The parameters that appear in the Wireless Security Settings group depend on your selections in these controls:

- Security Mode
- 802.11 Mode
- AP, Ethernet Bridge, Bridging Client, or Client radio modes

The parameters listed in the *Wireless Security Settings* group automatically change when you make a change in any of these parameters. The **APPLY CHANGES** button should only be clicked once all changes have been made.

Parameter	Description
Security Mode	Specifies the security mode for the radio. **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 *3.3.2.1 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. **WPA3 -** The latest security protocol that is mandatory for operation in the 6 GHz band. **WPA/WPA2 -** Allows connection to a peer device using WPA if the peer does not support WPA2. **WPA2/WPA3 -** Allows connections to APs in the 5 GHz band that only support WPA2, as well as connections to APs in the 6 GHz band using WPA3. **Note:** A connection with a peer will always use the highest (strongest) mode that is common between the devices. If the security modes supported by the peer do not include the mode(s) set in this control, then a connection is not attempted between the peers. **Note:** APs operating on 6 GHz channels only advertise WPA3. Therefore, an ELXM-SW6 client set to WPA or WPA2 will never pick a 6 GHz AP as a Parent candidate.
Encryption	Specifies the encryption method for the radio. AES is the preferred encryption mechanism as it is the most secure protocol supported by the 802.11 standard. Support for legacy methods that are not secure is no longer available. **AES** is the only Encryption method supported and is used with all Personal and Enterprise modes.
WPA phrase	Specifies the WPA passphrase of between 10 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 10 and 63 normal keyboard characters. As an aid to creating a secure passphrase 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 passphrase used results in a dark green background indicating the highest strength. 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 Enterprise Mode Settings

When you select one of the *Enterprise* modes in the *Security Mode* group, there are two sets of controls:

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

3.3.2.1.1 Enterprise Security Parameters in AP mode

In Enterprise mode, the radio authenticator communicates directly with the RADIUS Server while it is relaying 802.1x frames received from an associating note's Supplicant. You must 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 this radio.
UDP Port	Specifies the UDP port number the RADIUS server is used to listen to Radius frames from this radio. The default port number used for the Radius protocol is 1812.
Secret	Specifies the pass phrase that was used when this radio was registered to the RADIUS server. This validates that the Radius frames received on either end are legitimate.

3.3.2.1.2 Enterprise Security Parameters in Bridge or Client Modes

When in Bridge or Client mode, the ELXM-SW6 Radio 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 radio 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. Like 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.

Parameter	Description
Authentication Method	Specifies the authentication method, sometimes referred to as the inner protocol. This defines the mechanism used to authenticate the Supplicant of the radio 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.
User Name	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 radio and provides controls to upload new certificates into the ELXM-SW6. For more information, see section *3.3.2.2 Certificate Management*. **Note:** The ELXM-SW6 Radio does not ship with any certificates installed.

3.3.2.2 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 Radio. There are two certificate types; a certificate from a 'Certification Authority' used to authenticate the RADIUS server to the radio supplicant, and device or client certificate created by the RADIUS server for the radio. The ELXM-SW6 Radio can hold one of each certificate type.

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

To configure the ELXM-SW6 radios with certificates

1 Obtain the required certificate files from your IT department.
2 Log into your radio. For more information, see section *3.1 Connecting to the Radio Configuration Interface*.
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 box to enter the certificate files.

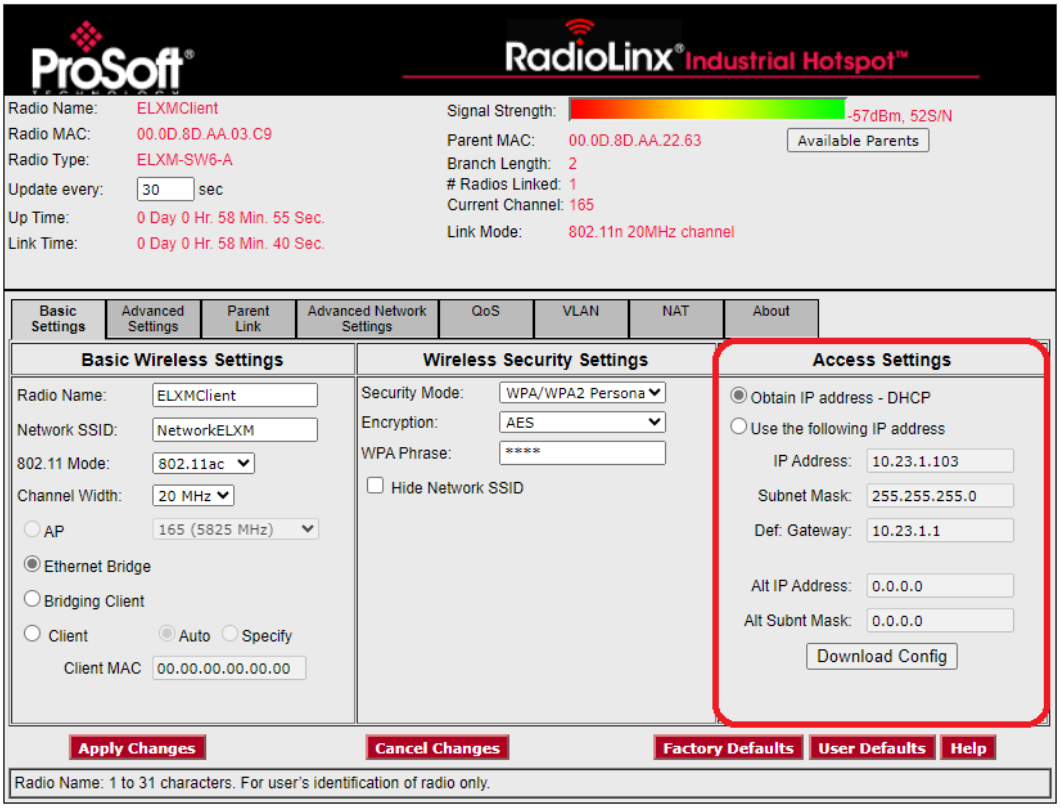


Parameter	Description
Certificate Type	Specifies the type of certificate that you are uploading. It is important that this is set correctly as the ELXM-SW6 Radio does not distinguish between certificate types in any other way. A CA Certificate is required for both **PEAP** and **EAP-TLS**. This is used 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	Select the certificate file to be uploaded from your local PC.
Don't Validate Server's Certificate	The radio does not validate the server's certificate.

6 Select the **CERTIFICATE TYPE**.
7 Click **CHOOSE FILE** to select 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 connect to the Master radio.

3.3.3 Access Settings

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



Parameter	Description
Obtain IP Address -DHCP	Select this if the radio is to automatically get an IP address through DHCP.
Use the following IP address	Select this to manually define IP address for the radio. 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.

To assign the IP address for your radio

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

3.4 Configuring Advanced Settings

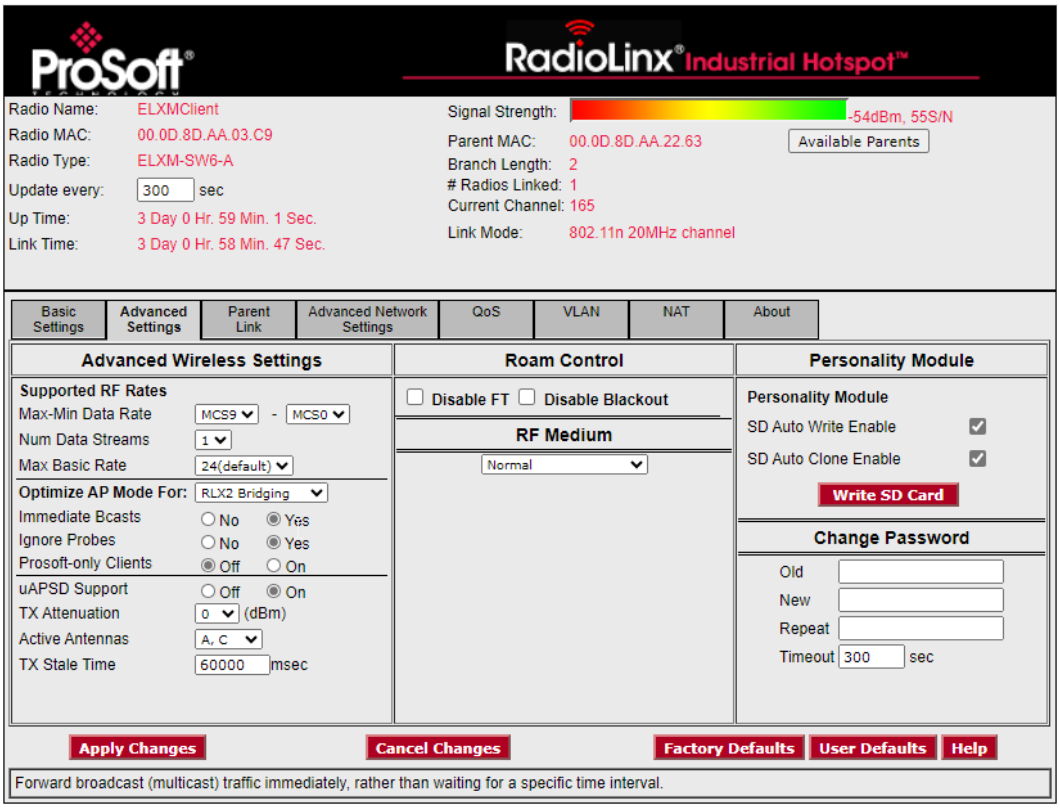
It is important to allow many industrial protocols to communicate properly over the ELXM-SW6 Radios. The standard 802.11 AP operation for transmitting broadcast messages is to accumulate them and transmit them on specific time intervals. This allows clients that are in power-save mode to wake up at the 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 allow you to configure the transmission rate and broadcast mode to optimize this radio's use on an industrial network.

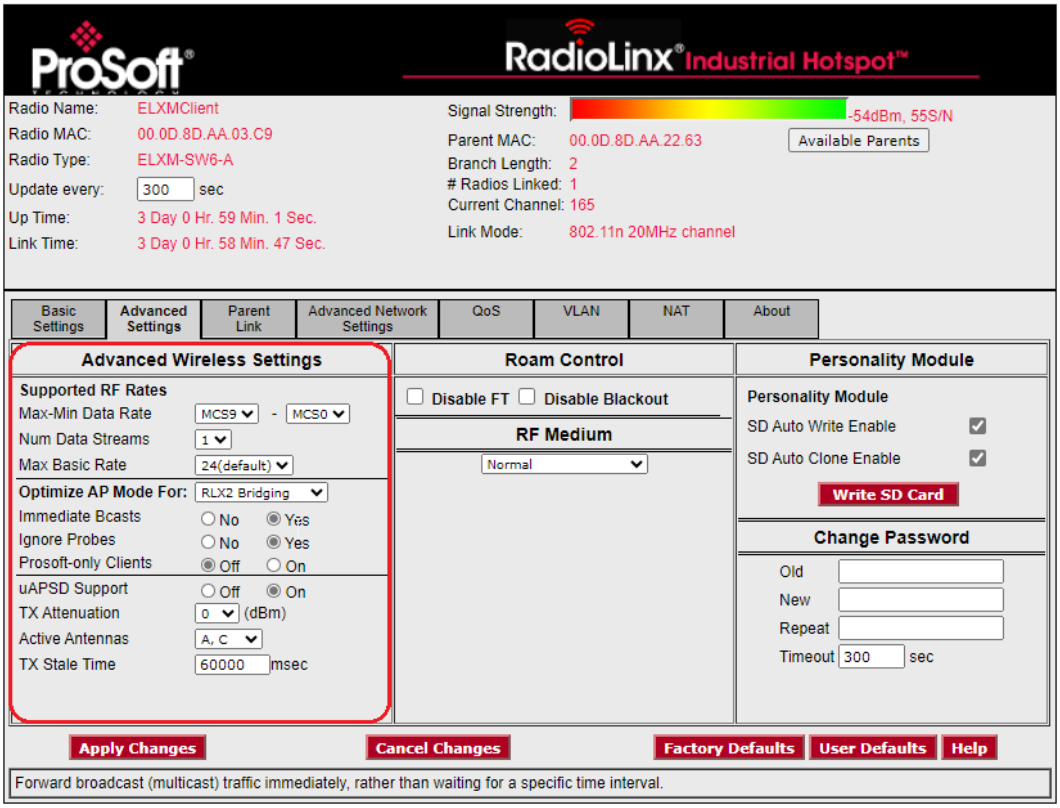
Advanced Settings include:

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



3.4.1 Advanced Wireless Settings

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



It is important to allow many industrial protocols to communicate properly over the ELXM-SW6 Radios.

The standard 802.11 AP operation for transmitting broadcast messages is to accumulate them and then transmit them only during 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 also allow you to configure the transmission rate and broadcast mode to optimize the radio's use of an industrial network.

Parameter	Description
Min-Max Data Rate	In AP Mode, the maximum and minimum data transmission rates, advertised by this radio 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 this radio 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-only Clients controls, for three specific interoperability scenarios when operating in AP mode. **3RD PARTY CLIENTS -** optimizes these controls to provide an infrastructure for 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 radio forwards broadcast/multicast traffic immediately, rather than waiting for specific time intervals.
Ignore Probes	If set to No, the ELXM-SW6 will respond to all Probe Requests that are received. If set to Yes, the ELXM-SW6 will only respond to probe requests that are specific to the radio's SSID and will ignore all general probes.
ProSoft-only Clients	If set to Off, the ELXM-SW6 will allow all 802.11 devices that have the correct security keys to connect to this Bridge. If set to On, the ELXM-SW6 will reject all connections from 3rd-party non-ProSoft wireless devices.
uAPSD Support	This determines whether uAPSD support (Unscheduled Automatic Power Save Delivery) is advertised in the ELXM-SW6's Beacons. When set to Off, connected client devices 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.

Parameter	Description
TX Attenuation	This determines the amount of attenuation that will be applied to the output power of the radio. 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. There are two options for the *Active Antennas* parameter: **A, C -** The default setting; used for a two-connector MIMO antenna. **A ONLY -** Used for one SISO antenna. In general, MIMO antennas give the best performance.
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 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.

3.4.1.1 802.11n 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

3.4.1.2 802.11ac Data Rates

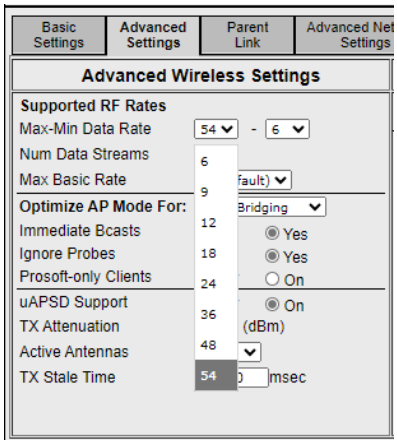
			802.11ac 20MHz, Mbit/s		802.11ac 40MHz, Mbit/s		802.11ac 80MHz, Mbit/s	
MCS Index	**Active Antennas**	**# Streams**	**800 ns GI**	**400 ns GI**	**800 ns GI**	**400 ns GI**	**800 ns GI**	**400 ns GI**
0	1 or 2	1	6.5	7.2	13.5	15.0	29.3	32.5
1	1 or 2	1	13.0	14.4	27.0	30.0	58.5	65.0
2	1 or 2	1	19.5	21.7	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

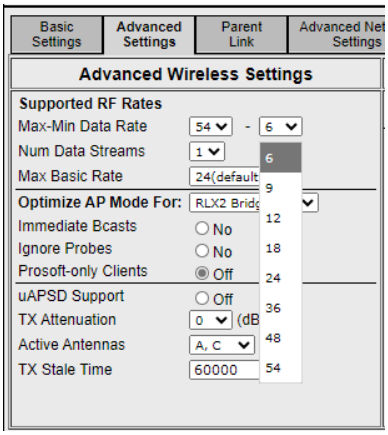
3.4.1.3 802.11ax Data Rates

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

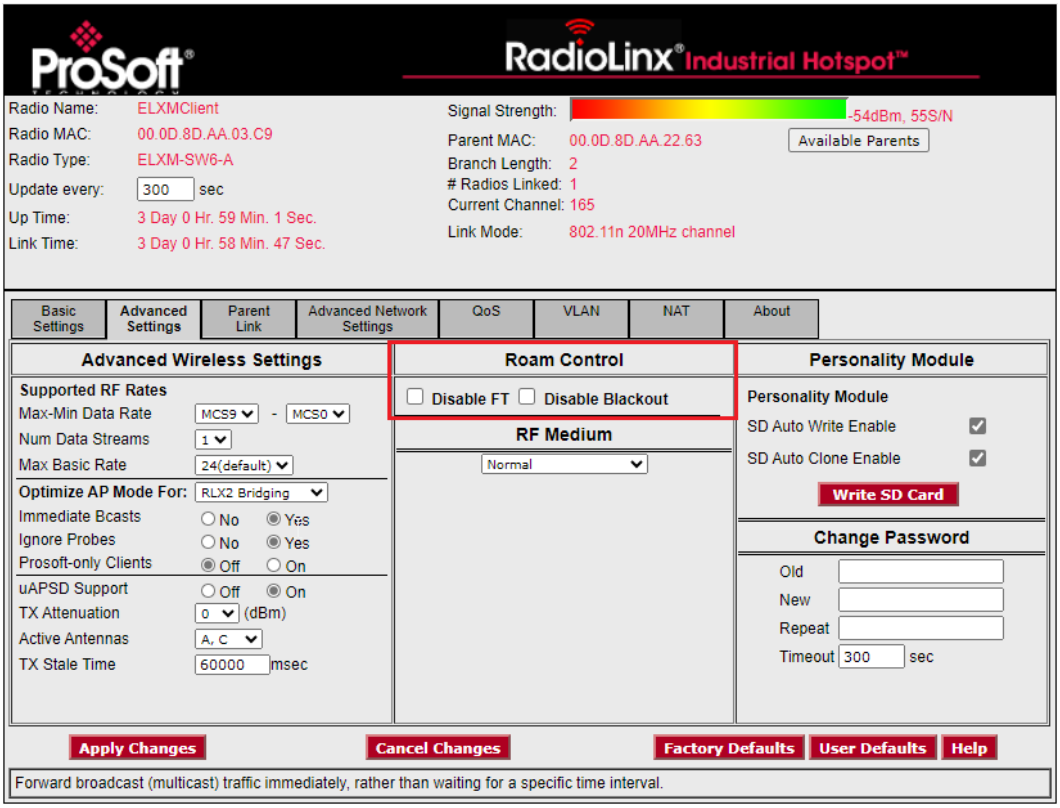
When the ELXM-SW6 is in 802.11a/g mode, the *Advanced Wireless Settings* group includes the following Data Rates:





3.4.2 Roam Control Settings

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



In roaming applications, a mobile platform equipped with an ELXM-SW6 radio roams from one AP radio's coverage area to another radio's coverage area. By default, a Client radio automatically roams 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 Radio 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. You can disable **FT ROAMING**, which results in normal non-FT Roaming.

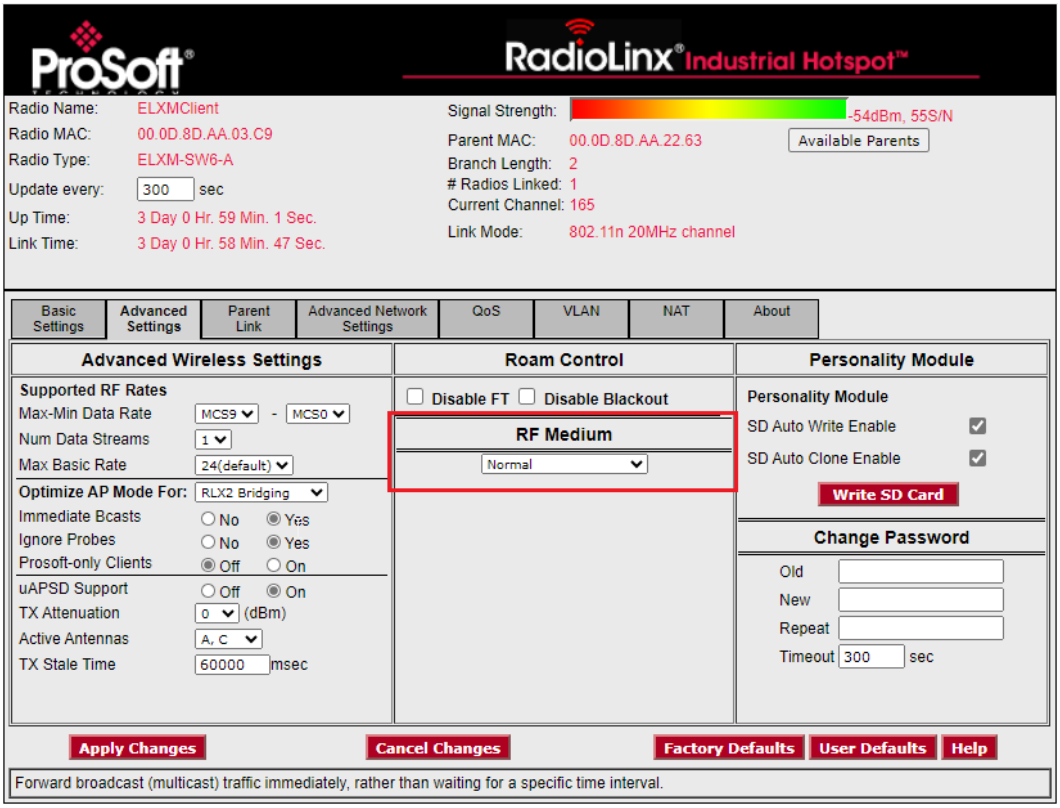
Parameter	Description
Disable FT	Rhis disables Fast Transition (FT) roaming in this radio. **Note:** With FT disabled, the roam duration could double, and roams are no longer 'hitless' as there may be some frame loss in the Parent-to-Child direction. FT should be enabled other than a few exceptional 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 has 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.

3.4.3 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.

For these scenarios, a special mode is used by the ELXM-SW6 Client. This mode requires the use of two separate antennas and can quickly 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.

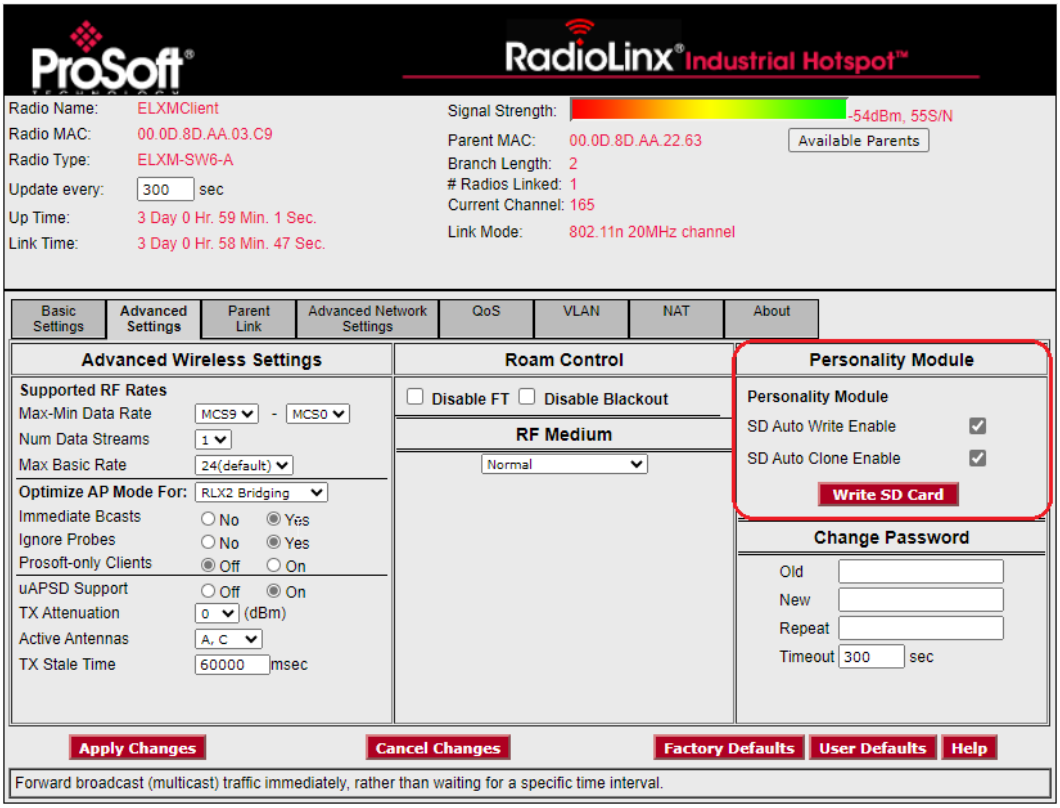
In the Client, setting to Discontinuous mode will also automatically result in the following configuration changes:

- 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, but the user is free to set a higher MCS rate that is lower 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 creates 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)	Select 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.

3.4.4 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. You can use the microSD card to save the radio's configuration. This makes it easy to replace the radio with a new radio by moving the microSD card from the old radio to the replacement radio. For more information, see section *2.7 Replacing an Existing ELXM-SW6*.

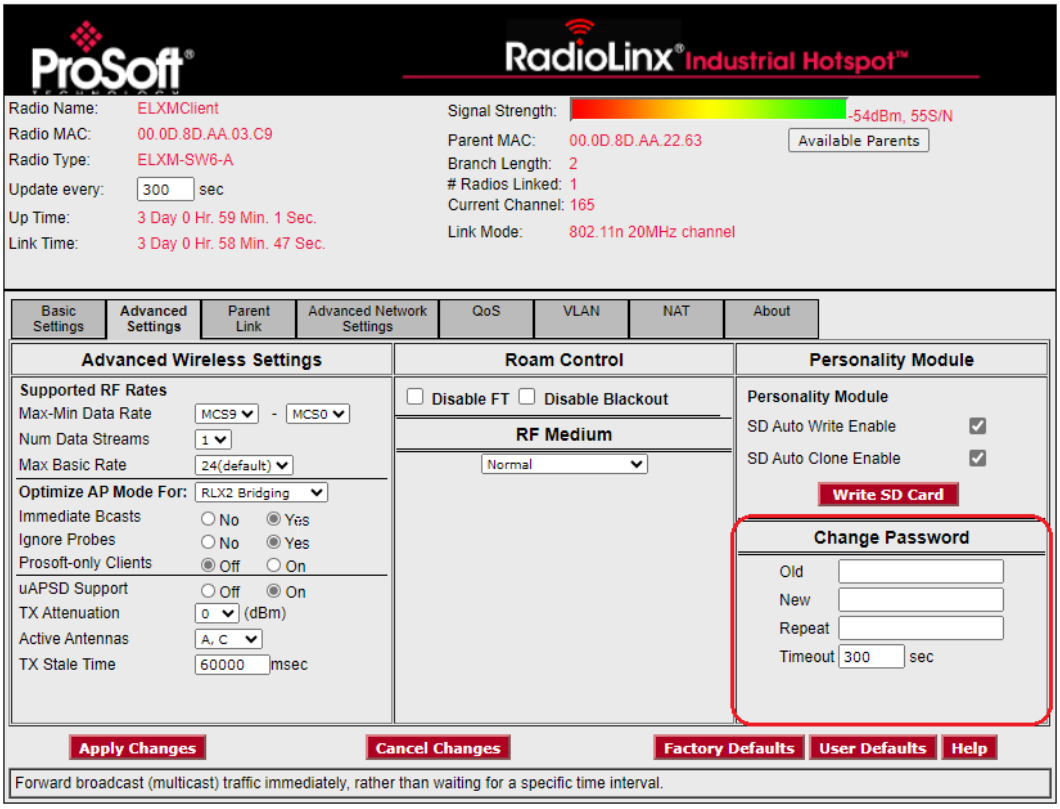


Note: The configuration files on the microSD card are stored in an encrypted binary format so sensitive data (e.g. passwords, encryption keys) cannot be read from the files.

Parameter	Description
SD Auto Write Enable	Select this check box to have the radio write a copy of its configuration to the microSD card whenever new settings are saved from the web configuration interface. The radio renames previous radio configuration files with a unique file name that allows you to audit changes made to the radio's configuration.
SD Auto Clone Enable	Select this check box to have the radio use the configuration from the microSD card when the radio powers up. • If a microSD card is present and has a configuration file that is different from the radio's current configuration, the radio uses the configuration from the microSD Card. • If the configuration on the microSD card matches the radio's configuration, or there is no configuration file on the microSD Card, then no action is taken. • If you insert a microSD Card into a running radio, and if the configuration file on the microSD Card is different from the radio's current configuration, the radio warns you by flashing the Signal Strength, MOD and NET LEDs. If you reboot the radio or cycle power to the radio, it uses the configuration from the microSD card. If you want to save this control as enabled (checked), either the microSD card slot in the radio must be empty, or you must 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 a microSD card when this control is already enabled, insert the microSD card and cycle power to the radio. • If this control is not enabled, enable and save the setting without the microSD card inserted (click **APPLY CHANGES**), then insert the microSD card, and then cycle power to the radio. **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 radio 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.

3.4.5 Changing Password Settings

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



To change the password

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 radio's webserver.

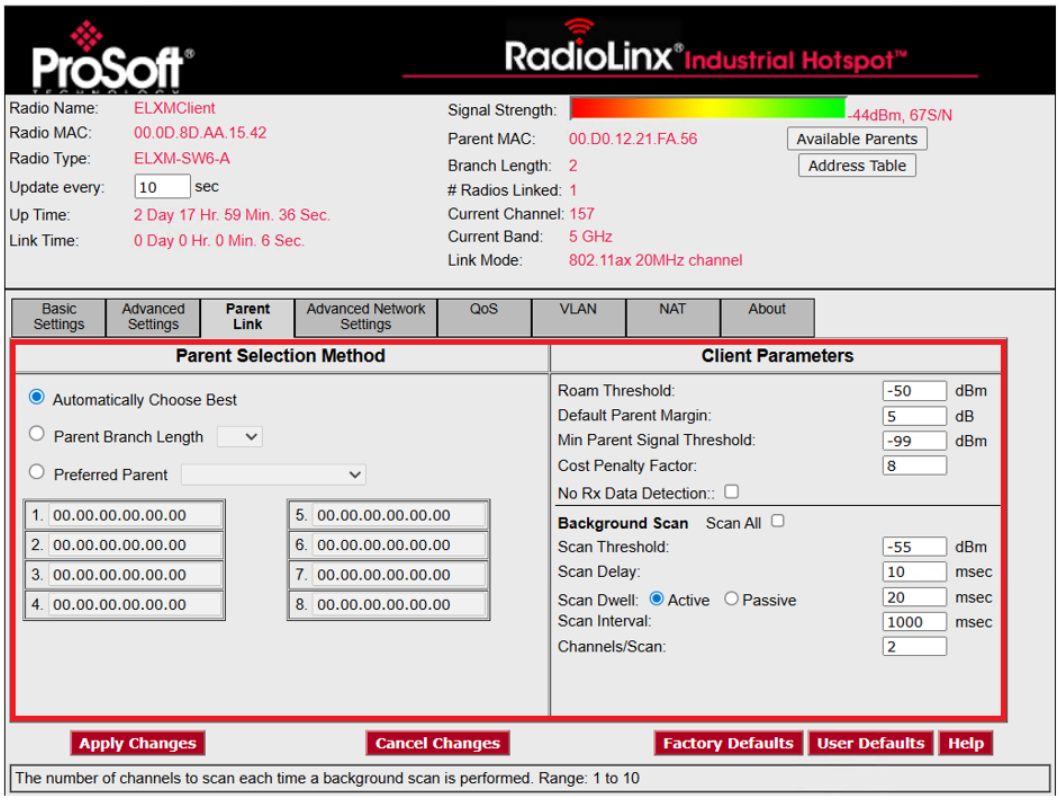
Note: Changing tabs and editing fields does not refresh this timer as those changes are local to the web browser. The radio only restarts the login session timer if a webpage is refreshed, or the top info pane updates its information, or an **APPLY CHANGES** is done.

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 Radio Status*.

3.5 Configuring Parent Link Settings

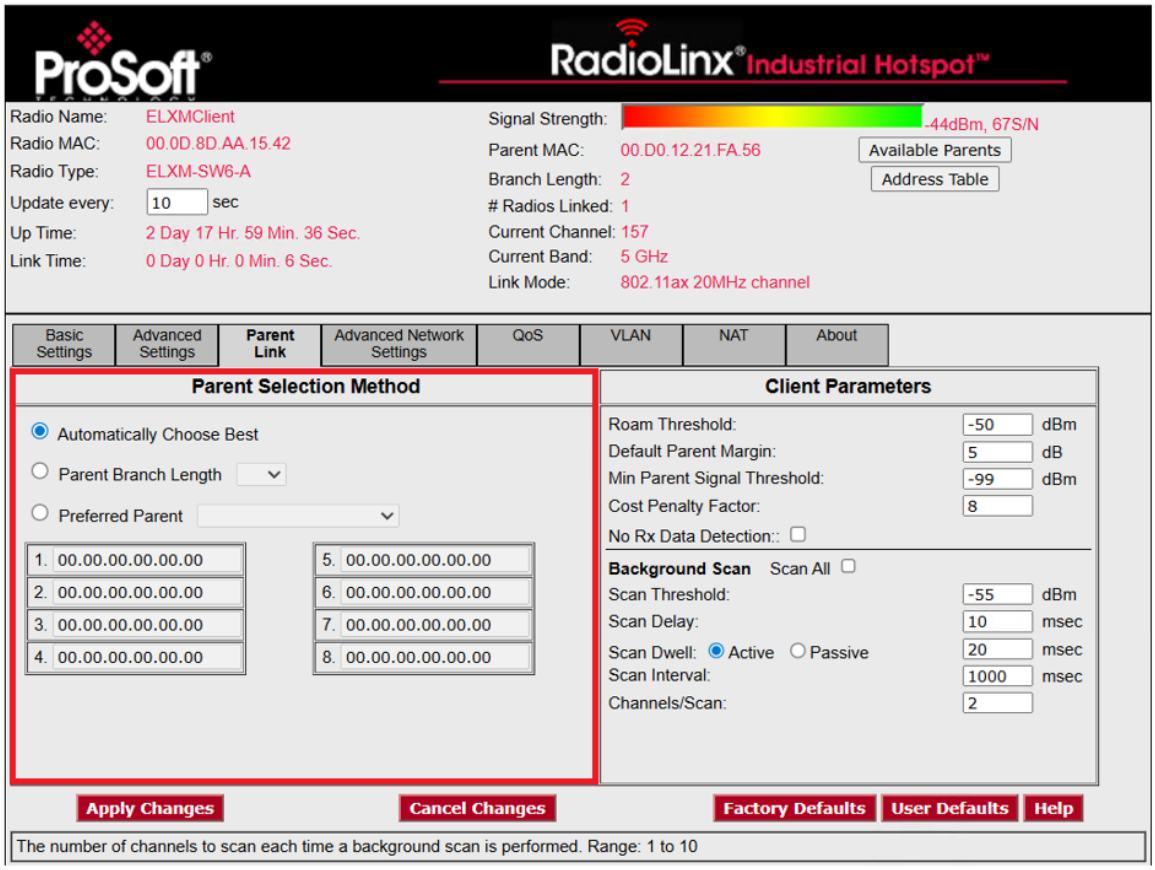
Use the *Parent Link* tab to specify how an ELXM-SW6 Client radio selects a Parent to connect to the network. Parent Link includes two groups:

- Parent Selection Method
- Client Parameters



3.5.1 Parent Selection Method Settings

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

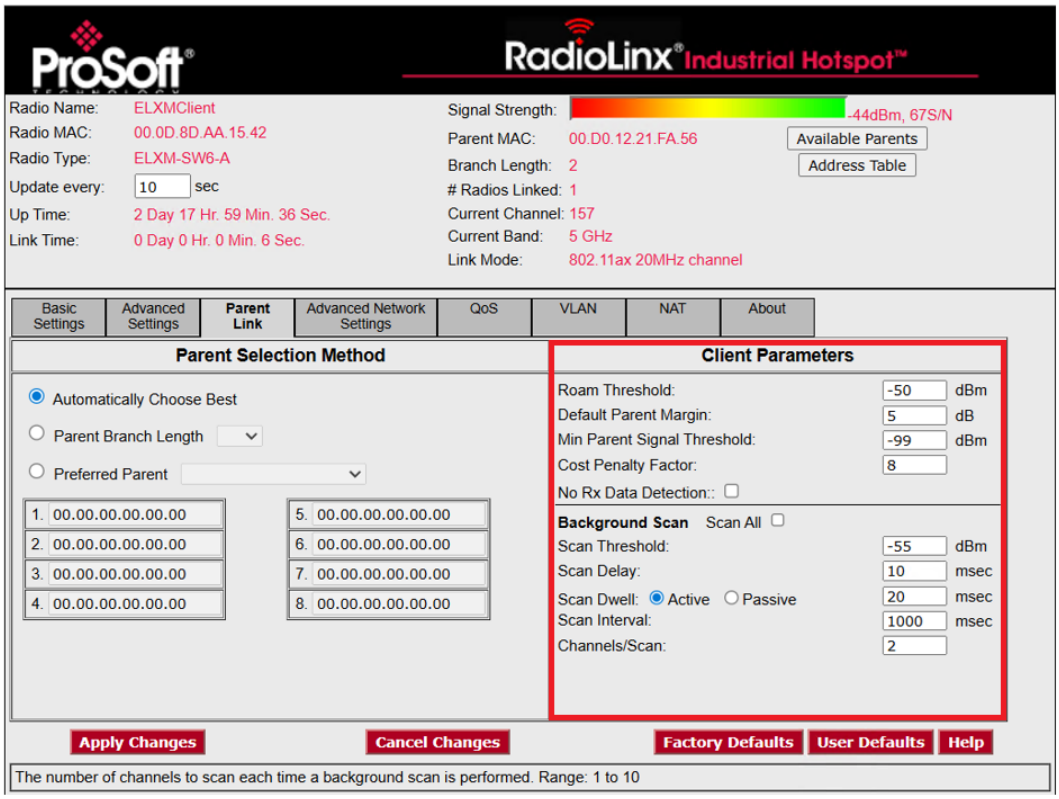


Parameter	Description
Automatically Choose Best	Calculates a "cost" metric for each possible parent radio that detects and selects the Parent radio based on the lowest cost. The radio's calculation includes: • RSSI - Stronger signals receive a lower cost. • Hop Count - Fewer hops from the AP radio is given preference and therefore a lower cost
Parent Branch Length	Calculates the branch length to other radios and chooses the Parent radio strictly by the number of RLX2-IHNF Repeater radios between this radio and the AP radio. • If you choose a branch length of 1, the radio links only to the AP radio. • If you choose a branch length of 2, the radio links only to a ProSoft 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 radio 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 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. You can specify a list of up to eight radios by entering the MAC addresses for each radio. The radio chooses its Parent radio based on your selection for **PREFERRED PARENT:** **BEST IN LIST -** The radio 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 radio 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 radio only selects a Parent radio from the list that is operating in the 2.4 GHz band. **5 GHZ PARENTS ONLY -** The radio only selects a Parent radio from the list that is operating in the 5 GHz band. **6 GHZ PARENTS ONLY -** The radio only selects a Parent radio from the list that is operating in the 6 GHz band. **5&6 GHZ PARENTS ONLY -** The radio only selects a Parent radio from the list that is operating in either the 5 GHz or 6 GHz bands

3.5.2 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 above which a stronger signal does not improve the quality of the link any further. For signals that are above that threshold, the radio only gives preference to Parent radios with fewer hops from the AP radio. Another way to consider this in Fast Roam applications is that the radio does not Roam to a new Parent radio at the same hop count level until its current Parent radio's RSSI goes below (weaker) than this value.

Default Parent Margin	Specifies a signal strength below which the radio will not select a different Parent radio. Use this in Fast Roam applications where the radio is on a mobile platform, or there is a lot of movement in the environment causing RSSI levels to fluctuate. The radio keeps its current Parent radio unless another Parent radio's RSSI is stronger than this value. The radio adds this margin value to the current Parent radio's RSSI prior to calculating its cost. It is desirable to Roam to a new Parent radio before losing the connection with the current Parent radio, since losing the connection results in data loss. • If you enter a value that is too small, it can lead to the radio rapidly switching back and forth between two Parent radios as the RSSI levels change. • If you enter a value that is too large, it can result in preventing a Roam until the radio moves out of range, even though a candidate exists that is better than the current Parent radio. The default value is 5 dB. • Use larger values (10-15 dB) to prevent false roams from occurring due to temporary RSSI inversions between the current Parent radio and another candidate. • Make sure that when Roaming that the RSSI difference between the current Parent radio and the new Parent radio is greater than this value.
Cost Penalty Factor	This parameter controls the amount of penalty that is added to the current parent link due to Tx Failures. 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 decision 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. A value of **0** uses the internal default of 8. A value of **1** will disable the feature. The maximum value accepted is 64.
No Rx Data Detection	This parameter enables detection of an interval with no received data from the Parent. This parameter is only supported in a Client mode and should only be enabled if the application results in a steady stream of data from the AP to the radio. Once enabled, any gap in received data will begin accumulating a penalty that is added to the current AP link. When this penalty is large enough it will trigger either a roam to a nearby AP or a re-Association to the current AP if no other APs are close enough, to re-establish the receive data stream. The recovery time can vary from 1 to 15 seconds depending on the relative signal strength of other APs nearby. If at any time a directed data packet is received from the AP, the detection mechanism resets and waits for the next period with no receive data to restart the penalty accumulation.

3.5.2.1 Background Scan

The *Background Scan* parameters group are used to modify the algorithm used by an ELXM-SW6 in 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 a background scan is about to start.
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 the background scan is complete, allowing it to send any data frames it has buffered since our signal in Step 1.

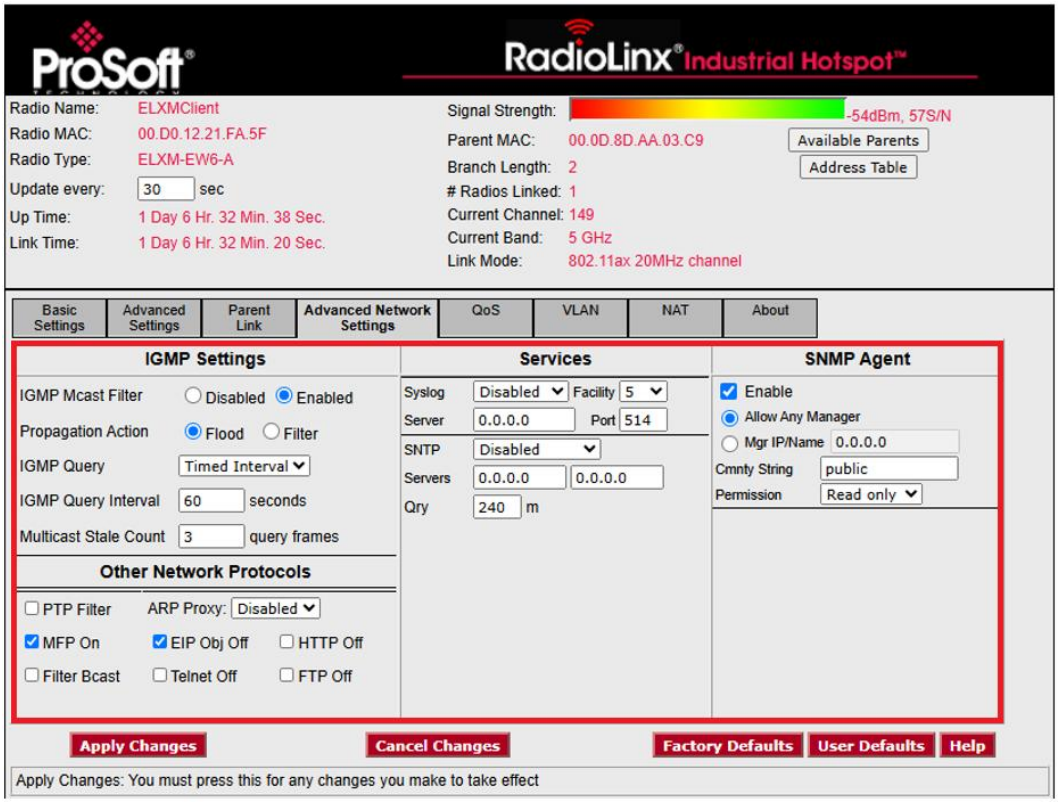
Parameter	Description
Scan All	When checked this control will force the ELXM-SW6 to include all channels in its background scan channel list, irrespective of information extracted from the AP Beacon's Neighbor Report. Check this control if the information from the AP Beacon isn't reliably indicating nearby APs that the ELXM-SW6 can roam to.
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 in this parameter shall disable 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 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 radio 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 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 *Scan 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 Clients 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.

3.6 Configuring Advanced Network Settings

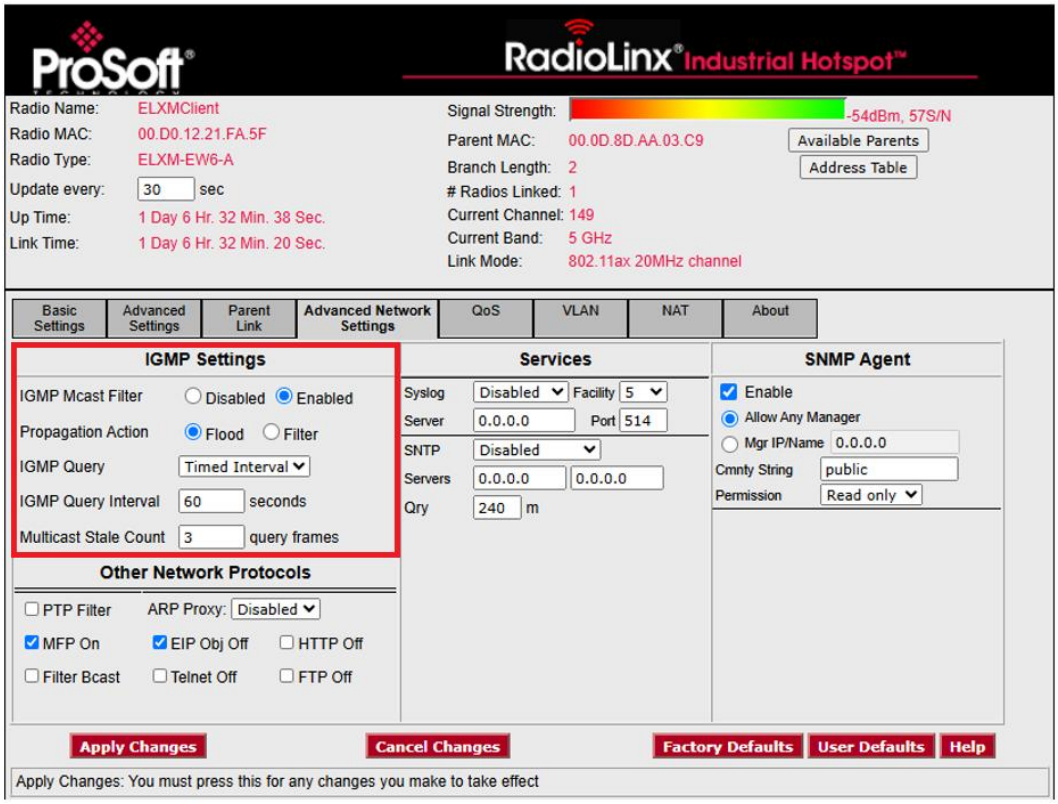
Use the *Advanced Network Settings* tab to specify the IGMP (Internet Group Management Protocol), STP (Spanning Tree Protocol), SNMP (Simple Network Management Protocol), and Location Services parameters for an ELXM-SW6 Radio. The *Advanced Network Settings* includes four groups:

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



3.6.1 IGMP Settings

Use the parameters in the *IGMP Settings* group to specify the Internet Group Management Protocol parameters of the ELXM-SW6 Radio.

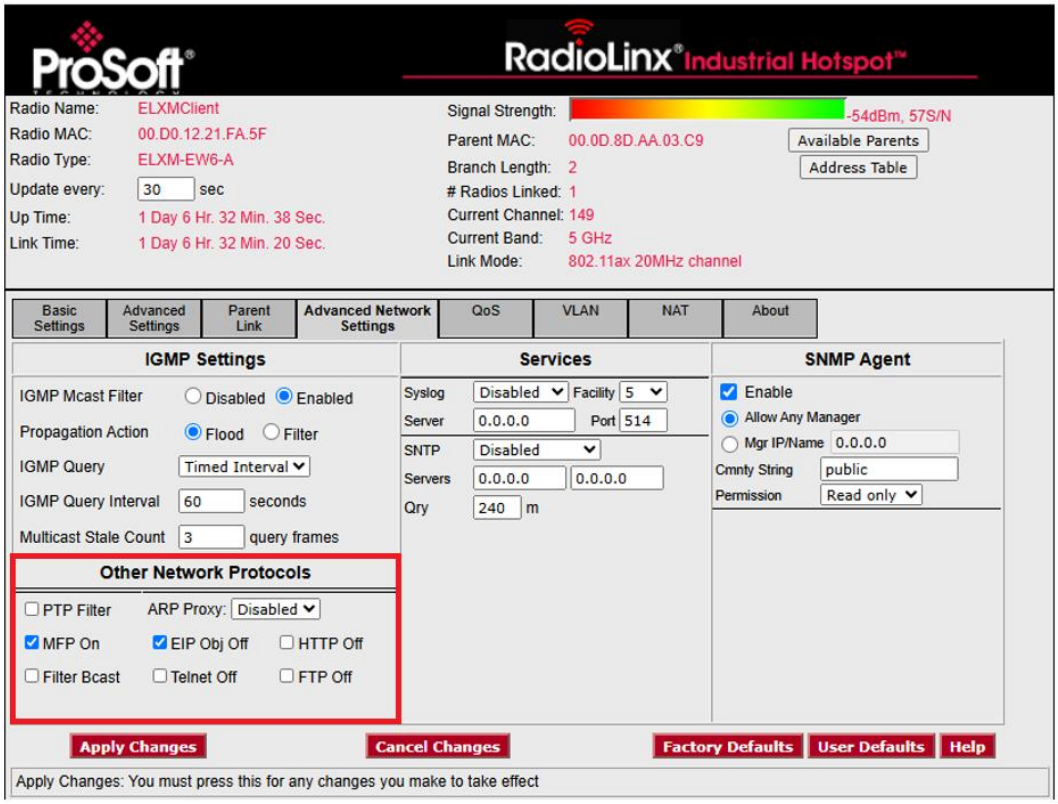


The ELXM-SW6 supports IGMP v1 and v2. The IGMP functions are enabled in the radios by default.

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 radio'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 this ELXM-SW6 if no response is received from the device.

3.6.2 Other Network Protocols

Use the parameters in the *Other Network Protocols* group to enable or disable actions taken on PTP or ARP packets received on the ELXM-SW6 Ethernet interface.



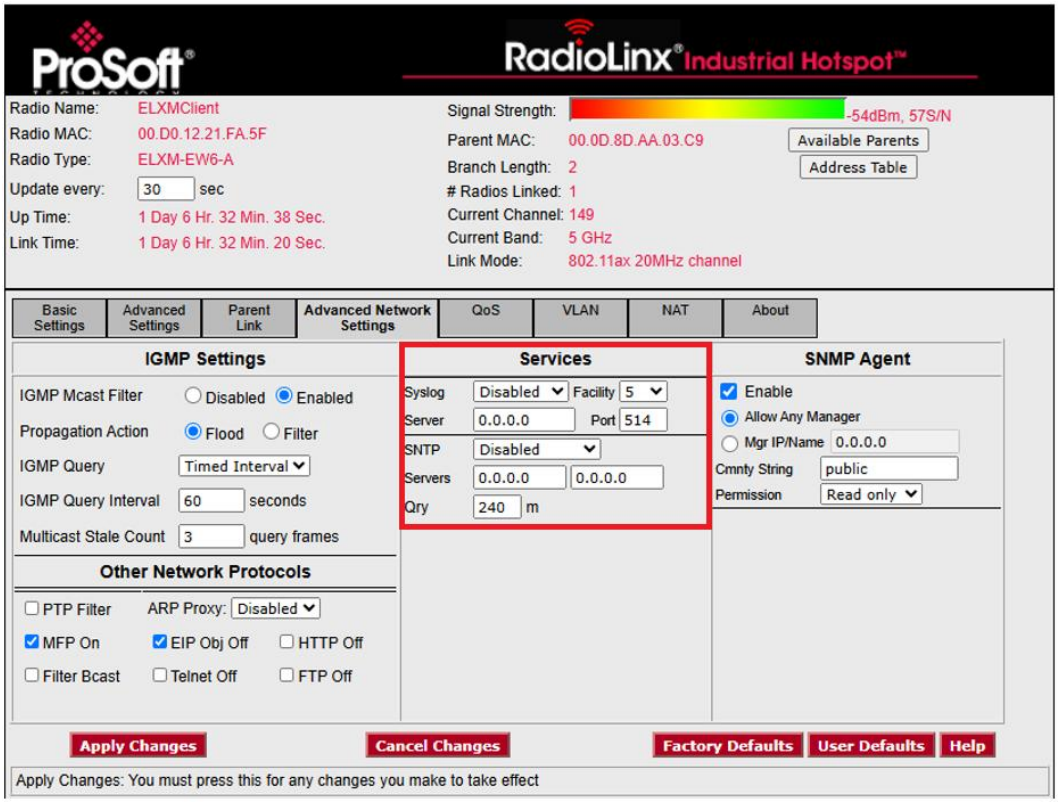
Parameter	Description
PTP Filter	Check this box to enable the PTP Filter feature. The Precision Time Protocol (PTP) is used in industrial networks to synchronize time between devices. Given the protocol uses multicast addressing, a PTP packet sent by one device is sent over every wireless link in that network. PTP is only needed amongst a set of local Ethernet connected ELXM-SW6s. 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 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 radio interface. **FILTER:** Arp Requests that are received on the Ethernet interface are always filtered and not forwarded to the radio 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 who's 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 radio 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-SW6 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 Off	Disables the EtherNet I/P agent in the ELXM-SW6. When checked queries to read the EIP Object classes are ignored. **Note:** The EtherNet I/P responses are not encrypted and therefore a Wireshark capture of these packets on any wired network would reveal their content 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 data. This control is provided for those customers that wish to shut down any interface that is not secure or is not required for their application. The factory default setting is 'checked' in firmware versions that are compliant with European RED 3.3 requirements.
Filter Bcast	Disables 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 Off	Disables 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. **Note:** The Telnet output is not encrypted and therefore a Wireshark capture of these packets on any wired network would reveal the logging output. This Telnet interface 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 users that wish to shut down any interface that is not secure or is not required for their application. The factory default setting is 'checked' in firmware versions that are compliant with European RED 3.3 requirements.

Parameter	Description
HTTP Off	This control is present in firmware versions that are compliant with European RED 3.3 requirements and is checked when reset to factory defaults. This checkbox can be used to enable legacy HTTP support for the ELXM-SW6's web server. **Note:** The use of HTTP is inherently insecure and should only be enabled to support any required legacy http client that does not support HTTPs. It is highly recommended that any client attempting to access the ELXM-SW6's web server should use HTTPS instead, which is always active and listening on port 443. When HTTP is disabled (default) any attempted access to the HTTP port 80, will result in a re-direct response from the ELXM-SW6's web server, redirecting the Web Browser to an **https://** link.
FTP Off	This control is present in firmware versions that are compliant with European RED 3.3 requirements and is checked when reset to factory defaults. This checkbox can be used to enable legacy FTP support for firmware uploads. **Note:** The use of FTP is inherently insecure and should only be enabled to support legacy management tools used to update ProSoft radios. It is highly recommended that these tools be updated to the latest version that uses a secure TLS connection to authenticate and transfer the firmware images. When FTP is disabled, any attempted access using FTP will be ignored.

3.6.3 Services

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



3.6.3.1 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 that occur during ELXM-SW6 operation are sent to an external Syslog Server that records the messages. These messages are time-stamped and can be reviewed at a later time to perform diagnosis and analysis of any system or wireless issues.

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 specified Server IP and Port number.
Facility	This control 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	Enter the IP Address or device Name of an SNTP Server into the first field. The Address or Name must be valid if SNTP is enabled otherwise an error pop up dialog will appear. Optionally an Alternate SNTP Server IP Address or Name can be entered into the 2nd field. If responses are not received from an SNTP Server it will switch to sending queries to the other SNTP Server. If an Alternate SNTP Server is not required, then the second field must be set with the IP Address **0.0.0.0** to bypass the IP Address checking. The SNTP protocol uses the standard port number 123.
Port	This control specified the UDP Port number that the external Syslog Server is listening.

3.6.3.2 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 message reflect 'real' time.

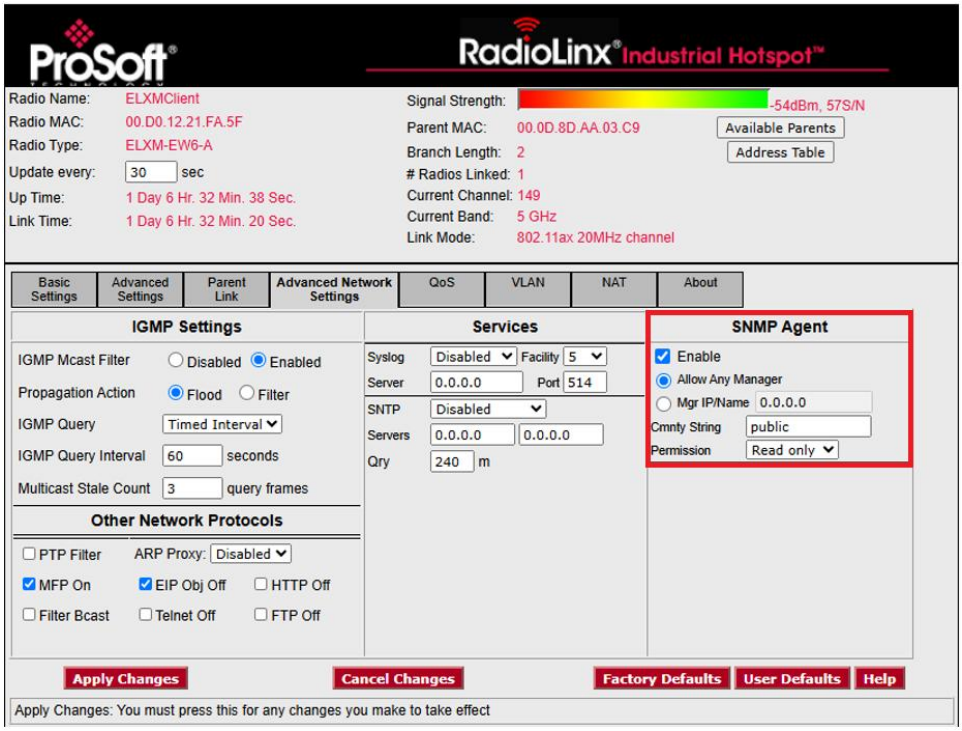
The ELXM-SW6 uses a SuperCAP to maintain its on-board real-time clock for up to 48 hours when power is removed. If power is removed for an extended time, on startup, the ELXM-SW6 initializes its system time to a built-in value representing when the firmware image was compiled. Since each ELXM-SW6 may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

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	Specifies the external SNTP Servier IP Address to which all SNTP Query messages will be sent. The SNTP protocol uses the standard port number **123**.
Qry	Specifies 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.

3.6.4 SNMP Agent

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



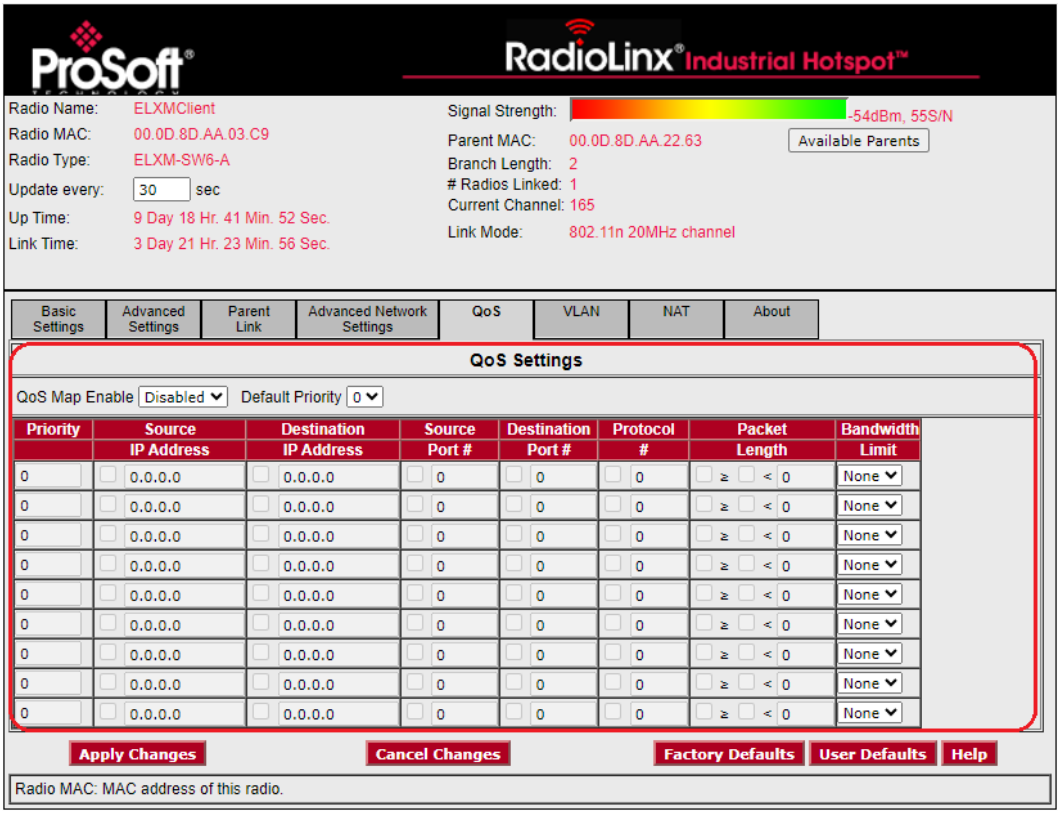
SNMP is a network management protocol that is often used with TCP/IP and Ethernet. It offers an alternative to using the radio web interface, and allows you to use an SNMP manager application to change radio settings and view diagnostics.

Parameter	Description
Enable	Select this check box to enable the following SNMP agent.
Allow Any Manager	Specifies that any user can change the radio configuration from any computer using SNMP.
Allow IP	Specifies that only an SNMP manager with a particular IP address can change the radio configuration. 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 this radio. **READ ONLY -** The SNMP manager can view but cannot change the radio configuration. **READ/WRITE -** The SNMP manager can view and make changes to the radio 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)
- The ELXM-SW6 also supports a selection of standard SNMP traps, including Cold Start, which the radio sends when it initializes.

3.7 Configuring Quality of Service (QoS) Settings

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



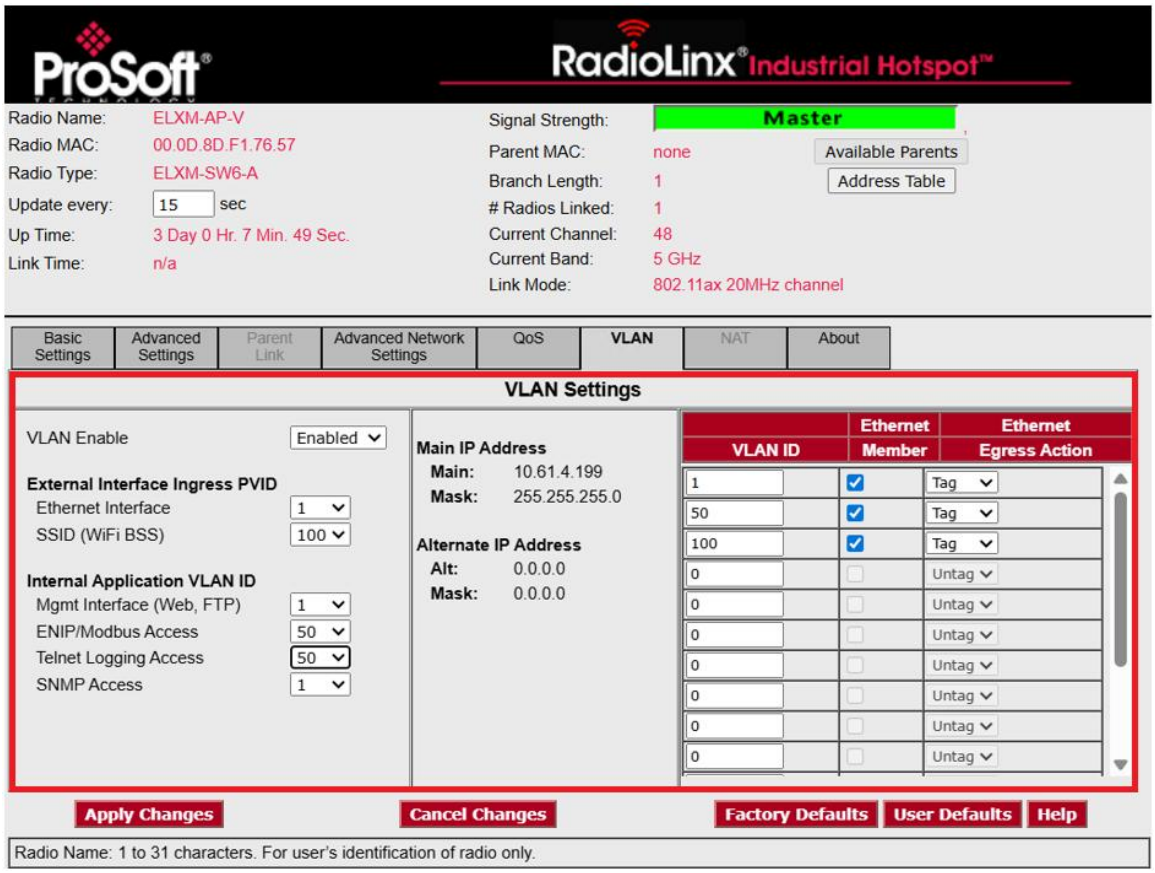
ELXM-SW6s prioritize frames using QoS for packets received already marked with a priority value. The *QOS* tab allows you to set the default priority for frames that the ELXM-SW6 receives without any priority markings. In addition, you can map a priority value to packets received without priority markings 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. Select *Enabled* before editing 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 radio 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. You must enter a packet length threshold. You must 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%

3.8 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-SW6s 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 radio itself, and the 802.11 BSS created by each AP.

You can configure the VLAN settings for the Ethernet interface on all ELXM-SW6s. You can only configure the VLAN for the Internal Application and SSID ports on a ProSoft AP radio. The 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 made 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.

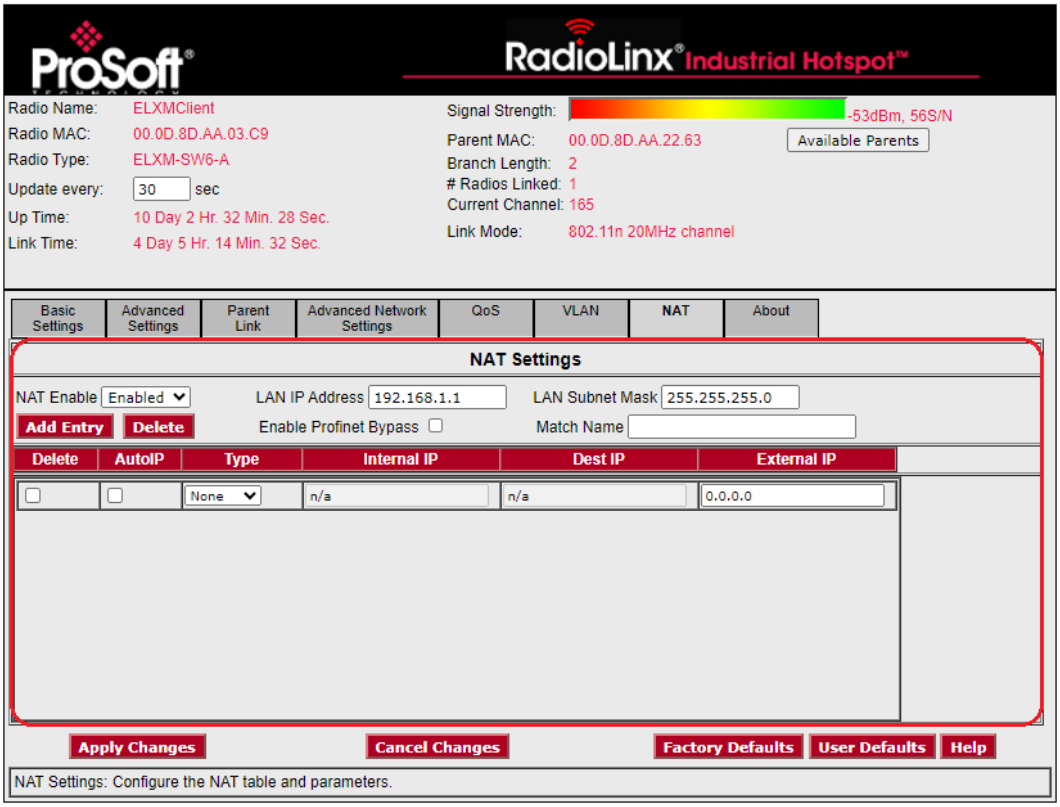
For networks that assign a different subnet on each VLAN, the ELXM-SW6 supports the configuration of a 2nd Alternate IP Address via the *Basic Settings* > *Access Setting* section of the ELXM-SW6 webpage. This allows the internal applications to be accessed with either IP Address if the packet is tagged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

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

Parameter	Description
VLAN Enable	Enables 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. You can configure up to 15 different VLAN IDs. **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 ELXM-SW6 Ethernet interface 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**.

3.9 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.

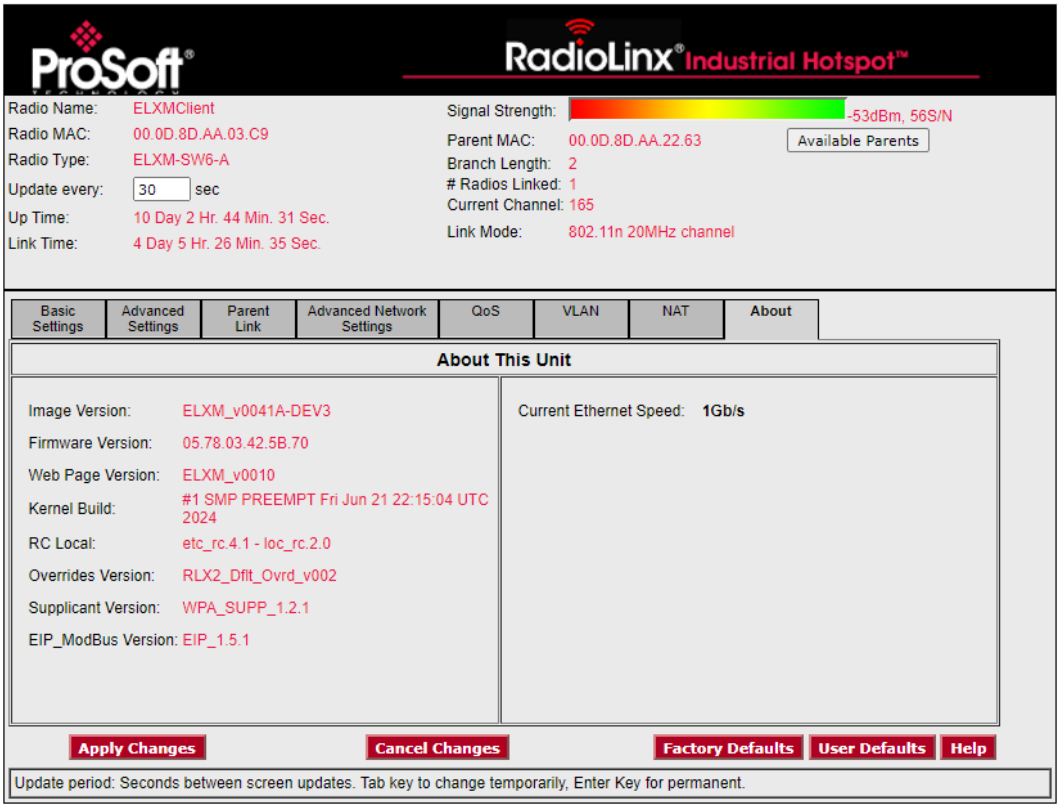
There are 2 types of NAT entries: *1:1 Src* entries and *1:1 Dst* entries. All devices on the internal network that wish to access or wish to be accessed from the external network must have a *1:1 Src* entry in the NAT table to translate their internal IP Address to an external IP Address. This means 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	Enables or disables 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. When 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 port. If NAT is disabled, then no Network Address Translation (NAT) occurs and the ELXM-SW6 operates in normal Ethernet Bridge or Bridging Client mode.
LAN IP Address	The LAN IP Address becomes 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 correctly set the subnet mask 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	This function allows 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 port whose PROFINET Name contains the *Match Name* value, will have its PROFINET packets bypass the NAT layer. To enable a PROFINET connection to be set up, 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	This function configures 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	This parameter is used to add a new entry to the NAT table. When used a new row appears at the end of the list in the table view. Up to 16 entries can be present in the NAT table. Attempting to add more will pop up an error message dialog. Once added 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 pressed.
Delete	This parameter is used to remove selected entries from the NAT table. When used 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.

3.10 About The ELXM-SW6

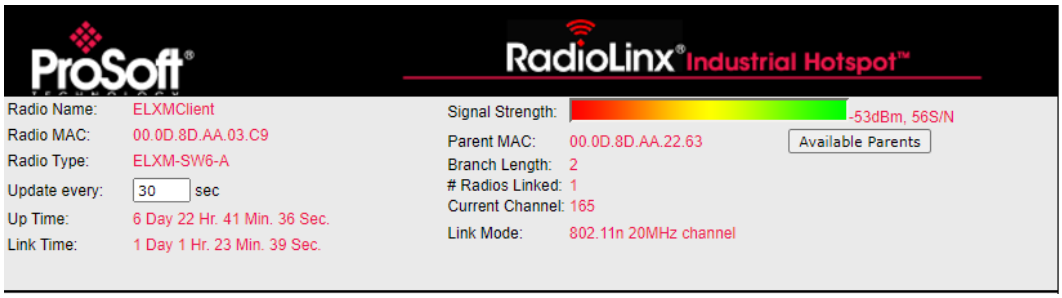
This tab displays the version of various modules that have been loaded and are running in the ELXM-SW6.



Parameter	Description
Image Version	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. It contains many sub-components.
Firmware Version	The main radio driver version number and is one sub-component of a Software Image.
Webpage Version	The version of the webpages that are available for management of the ELXM-SW6 via its web interface.
Kernel Build	Identifies when the OS kernel running in the ELXM-SW6 was built.
Overrides Version	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	The version of the WPA Supplicant that is responsible for Enterprise level Security and used for the Security exchange during FT Roaming.
EIP-Modbus Version	The version of the EIP/Modbus Agent that allows observation of radio status and parameters using EtherNet I/P 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 ensure the network is working properly:



- **Signal Strength**: This displays the radio'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 other parameters on this display are Read-only.

Tip: You can display the help topic for any parameter by clicking the parameter name.

You can 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
- 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 illuminate, there may be a problem with the Ethernet cable. Verify that the cable is plugged into the ELXM-SW6 at one end, and to an Ethernet hub, 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 ELXM-SW6 and the injector and 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 direct connection to a PC.

4.2 LED Display

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

LED	Description
POWER	● Booting up ● Fully operational This tri-color LED turns amber when power is first applied. The power LED then turns green, indicating the radio is operational.
ACTIVITY	⬬ Transmitting or Receiving data over the wireless interface
SIGNAL STRENGTH	● Booting up – will turn on for ~ 1 sec and then turn off. ● ● ● Blinks if SD card inserted with new configuration. This is for all radio modes. Radios in AP mode: ○ ● ○ No radios linked ○ ● ◗ One or more radios linked (right LED blinking). Radios in Repeater or Client mode: ○ ○ ○ No Signal / Not connected to an AP ● ○ ○ Radio linked, Poor Signal ● ● ○ Radio linked, Fair Signal ● ● ● Radio linked, Good Signal

The following LEDs should illuminate when power and Ethernet cables have been applied to the ELXM-SW6.

- The POWER LED should be green.
- The LINK LED on the Ethernet connector should indicate a valid wired link. This LED is located at the bottom of the Ethernet RJ-45 connector and is marked LINK
  - OFF = 10 Mb/s
  - ON = 1000 Mb/s
  - BLINK = 100 Mb/s
- The ACTIVITY LED on the Ethernet connector should blink occasionally indicating Ethernet transmit and/or receive activity.
- The wireless ACTIVITY LED below the POWER LED should start to blink occasionally.

For ELXM-SW6s in Bridge or Client modes, all three SIGNAL STRENGTH LEDs blink just after the ELXM-SW6 links to the AP radio but 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 an ELXM-SW6 Radio to Factory Defaults

If you lose the password to an ELXM-SW6, you cannot change the ELXM-SW6 settings. You can reset the ELXM-SW6 to restore the default password, but the ELXM-SW6 loses all the configuration settings and returns to the 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.



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 and the ELXM-SW6 continues its power up initialization.
6. You can now 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 the default operational settings that the user had previously loaded into the ELXM-SW6 using the IH Browser.

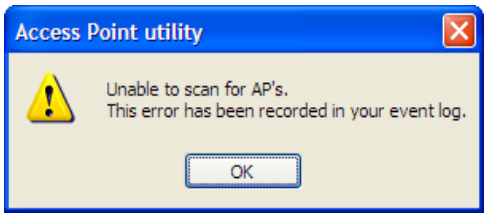
7 Power up the ELXM-SW6.
8 Locate the **Reset** button.



9 Once the ELXM-SW6 is running, insert the end of a paperclip or similar device into the hole to press the **Reset** button.
10 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.
11 Letting go of the **Reset** button will revert the ELXM-SW6 to a User Default configuration that had been previously stored on the ELXM-SW6 using the IH Browser and will immediately reboot to operate with those User Default settings. The Power, I/O and signal LEDs all flash amber 4 times, indicating 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 for ELXM-SW6s and no valid network connection exists on the PC (wired or wireless).



To correct this error

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 Security

This chapter contains security recommendations for the ELXM-SW6. It covers the following lifecycle phases:

- Secure installation
- Secure commissioning
- Secure administration and operation
- Secure maintenance
- Secure decommissioning

A secure device can help maintain the security and availability of the network.

5.1 Scope

This chapter covers the recommended device security measures throughout the lifecycle of the device. These recommendations include:

- How to achieve defense in depth for the device
- How to harden the device
- How a specifically configured device can help achieve defense in depth for the system
- How a specifically configured device can help harden the system

A network device is part of a superordinate system. Therefore, the device and the system are interdependent. The system lifecycle and the requirements of the system for defense in depth are outside the scope of this document. References to the system lifecycle are made only if necessary, and only for informational purposes.

For the network, additional planning and implementation steps may be necessary. For example, an L3 network plan may be needed in addition to the VLAN plan mentioned in this document. The L3 network plan and the VLAN plan are both outside the scope of this document.

5.2 Defense in Depth

Defense in depth is a strategy that employs various independent security measures to guard an asset under consideration against specific attacks.

A system that employs defense in depth first confronts an attacker with a particular barrier. If an attacker overcomes this barrier, the system presents another barrier of a different type. A minimum of 2 barriers of different types shall guard any system asset under consideration. This layered security approach is considered best practice. It potentially demoralizes an attacker while taking the imperfection of real-world security barriers into account.

5.2.1 Defense in Depth vs. Hardening

In comparison to hardening, defense in depth is a more selective and structured approach. Defense in depth employs a specific subset of all conceivable security measures.

Hardening can be characterized as defense in broad. It aims at closing as many weaknesses in any barriers as reasonably possible. A strategy for hardening may include the concepts "least necessary functions" for the device and "least necessary privileges" for user accounts.

Develop a strategy for defense in depth first, then complement it by hardening.

For more information about secure installation recommendations, see section *5.4.1 Secure Installation Location*.

5.2.2 Responsibilities

Defense in depth as well as hardening need planning, implementation and maintenance. It is the responsibility of the system operator to perform these steps.

It is recommended to consider all security measures given in this document, and to select those that are most relevant for the actual situation.

5.2.3 Example

ID	Barrier	Description
	System Level	
1	Internet Firewall	An attacker must overcome the internet firewall to gain access to the company Intranet.
2	Industrial Firewall	An attacker must overcome the industrial firewall to gain access to the industrial network. The industrial firewall separates the industrial network from the company Intranet.
3	Dedicated device management VLAN	An attacker must overcome VLAN restrictions to snoop packets like unknown unicast frames of device management traffic.
	Device Level	
4	Secure management protocols	An attacker must overcome encryption to snoop packet contents.
5	Non-default user account names[1]	An attacker must guess or discover the actual user account names.
6	Non-default passwords[2]	An attacker must guess or discover the actual passwords.
7	Specific, restricted account privileges	An attacker must guess or discover the administrator account credentials to read privileged data or manipulate device settings.

[1] Dedicated user account names can be device-specific and can be deliberately chosen to be non-descriptive.

[2] Passwords can be specific to a certain access protocol (for example HTTPS or SNMPv3) and can be device specific.

5.3 Impact of the System Lifecycle to the Device Lifecycle

A network device is a component in a superordinate system. The system lifecycle determines parts of the device lifecycle. A system lifecycle involves a planning phase. The decisions taken in the planning phase affect the device lifecycle directly or indirectly.

Typical decisions during system planning include:

- The physical position of the device, for example, its installation location and environment
- The logical position of the device, for example, the security zone
- The requirements of the system for defense in depth

5.3.1 VLAN Plan

VLANs are a software-configurable concept to segregate a LAN (layer 1) into separate Virtual LANs (VLANs) on layer 2. Advantages include the separation of data packets belonging to different VLANs. The separation also applies to flooded multicast, broadcast, and unknown unicast frames. This helps confidentiality besides helping reduce the network load on layer 1.

A VLAN plan is a prerequisite for a secure configuration of the device and in turn for the security and availability of the system. Create a VLAN plan that segregates the network on layer 2. A dedicated management VLAN can be a barrier component in the defense in depth strategy.

For simple networks, a VLAN plan and the configuration of VLANs may be considered unnecessary from a functional perspective. However, VLANs are recommended from a security perspective.

Note: For the network, additional planning and implementation steps may be necessary. For example, an L3 network plan (outside the scope of this document) may be needed in addition to the VLAN plan.

5.4 Impact of Device Requirements on System Planning

Some requirements of the device have an impact on the system lifecycle phases and system planning.

Topics of this interdependence include:

- A secure installation location, including the following aspects:
  - Device availability: Power supply, power budget, and data link redundancy
  - Device and port LEDs
- The detailed physical device security requirements
- The user account policy parameters the device offers:
  - For the login policy
  - For the password policy
- VLAN ID restrictions arising from certain redundancy protocols: VLAN IDs ≥2 for payload traffic and device management.

5.4.1 Secure Installation Location

Refer to *Appendix A - Radio Hardware* for a suitable physical installation location.

Select a location that offers appropriate device security by restricting physical access:

- Install the device in a facility where only authorized personnel have access.

5.4.1.1 Device Availability

Device availability can be an important base for the security of the superordinate system. Check that the following device availability requirements are met as needed:

- Provide redundant power supply
- Provide an adequate power budget
- Provide data link redundancy. For wireless Client devices ensure the wireless infrastructure has enough redundancy such that the client is always within range of at least 2 Access Points.

5.4.1.2 Device and Port LEDs

The device and port LEDs show important information about the device state and the port states.

To prevent information leakage, consider the following security aspects as needed in addition to the secure installation location:

- Install the device in a cabinet with an opaque door.
- Cover or obstruct the LEDs with a removable cover.

5.4.2 Dedicated User Account Login Policy

Given its function is dedicated to bridging data packets to a peer device, the device has a simple login policy. There is only one Login Role and Account, since there is no reason to access its web interface other than to make configuration changes.

Note: Selection of a 'strong' password is highly recommended, as that is one layer in the Defense in Depth strategy. Use the following guidelines when selecting the password to use for the device.

5.4.3 Password Strength

The device provides feedback as the user enters a new password by changing the background color of the edit box. The color changes from Red (weak), to Yellow, to light Green, to dark Green (strong), using the following policy:

- Minimum password length of 10
- Must contain both uppercase and lowercase characters
- Must contain one or more digits
- Must contain one or more special characters

Note: The default password must be changed on the first login. It is recommended to plan an overarching password policy when selecting a password to be saved on each device.

5.4.4 Dedicated Logging Policy

Configure device logging settings:

- Assign the required logging destinations.
- Assign the required syslog facility level.
- Enable SNTP to provide real-time timestamps in syslog messages.

Note: It is recommended to plan an overarching device logging policy and apply it to each device.

6 Device Security

This chapter covers the device security throughout the lifecycle phases of the ELXM-SW6.

6.1 Prerequisites

It is assumed that the following system planning steps have been addressed, including:

- Suitable physical location for the devices
- Creating a dedicated account password policy

6.2 Recommended Installation Sequence

The device security lifecycle phases in a practical order are:

- Choice of an installation location
- Initial software update
- Initial security configuration
- Possible hardware modification for security
- Initial device installation
- Operation
- Maintenance
- Decommissioning

Note: Depending on needs of the system, the work steps can be performed in a different sequence.

6.2.1 Reasons for the Recommended Installation Sequence

Performing the initial configuration and the initial software update before the initial device installation can have the following benefits:

- The required resources, for example, prepared configuration files and device labels, may be more conveniently available in an office location.
- Time-consuming steps like software updates can be performed in parallel.
- Associated devices, for example, devices participating in a ring redundancy, can be configured contiguously.
- The remaining work steps in the field require less time.

6.2.2 Recommended Preparation for Installation

The following recommendations can help reduce the initial effort and save time:

- Decide which device software release to run on the devices.
- Download the selected software files.
- Prepare device configuration files based on the network plan.
- Prepare device labels.

Note: It is recommended to use the latest available release of the device software.

6.3 Choice of a Secure Installation Location

Refer to *Appendix A - Radio Hardware* for a suitable physical installation location. The device's function usually dictates the installation location, e.g. inside an AGV, or on a roof support if it is being used as an Access Point.

Check that the following device security requirements are fulfilled if possible or applicable:

- Install the device in an area that only authorized personnel have access.
- Install the device in a cabinet to which only authorized personnel have access.
- Install the device in a cabinet with an opaque door.

6.3.1 Device Availability Requirements

Device availability can be an important base for the security of the superordinate system. Also consider implementing measures that increase device availability.

Check that the following device availability requirements are fulfilled if needed:

- Provide an adequate power budget.
- If in a wireless client mode, provide adequate overlap of coverage by the wireless infrastructure.

6.3.1.1 Power Supply Power Budget Requirements

Refer to *Appendix A - Radio Hardware* for the power requirements of the device. Check that the power requirements are fulfilled if needed:

- One single power supply can deliver power for all the connected devices.

6.4 Software Update

The following description applies to:

- The initial software update for a device out-of-the-box.
- A software update as part of operation or maintenance.

Check if an updated release of the device software is available at: www.prosoft-technology.com.

Note: To check the running software release on a device that does not yet have an IP configuration, it is recommended to use the IH Browser Windows application. For more information, please see: *RadioLinx IH Browser - ProSoft Technology, Inc*.

To update the software on the device, management access to the device is needed. At the first login, the device requires the default password to be changed. Use a dedicated password according to the password policy.

If the device software is to be updated:

1. Back up the device configuration.
2. Update the device software, using a secure mechanism.
3. The new software will take effect when the device automatically reboots.

Note: It is recommended to regularly check for device software updates and use the latest available release. A new release of the device software can provide security improvements or benefits like new security-related device functions.

6.5 Security Configuration

The following description applies to:

- The initial security configuration for a device out-of-the-box.
- Changes in the security configuration as part of operation or maintenance.

To save time and effort with several such devices in the network, perform the following security configuration steps by loading a prepared configuration into the device using the IH Browser management tool.

At the first login with the default password, the device requires the password to be changed. Use a dedicated password according to the password policy.

Perform the following steps as needed:

- If using WPA2 or WPA3 Personal encryption, enter the Passphrase that was selected for the wireless network. The Administrator should ensure the Passphrase strength is observed. For more information, see section *5.4.3 Password Strength*.
- Preferably 802.11 Management Frame Protection should be enabled.
- Disable insecure management protocols.

When the device configuration is complete:

- If configuration was done manually, it should be documented or backed up using the IH Browser management tool.
- Include other device-related data like private keys.

6.5.1 Disable Insecure Management Protocols

By default, the following insecure management protocols are disabled and must be manually enabled via configuration settings on the web interface. Private data in the device consists of passwords and the WiFi Passphrase. Using these criteria the insecure interfaces are subdivided into two groups:

- Interfaces that expose private security data:
  1) FTP (default: disabled)
  2) HTTP (default: disabled)

- Interfaces that do not expose private security data:
  - SNMPv2 (default: disabled)
  - Telnet (default: disabled)
  - EIP Agent (default: disabled)
  - IH Browser interface (default: enabled)

It is highly recommended to only use the secure HTTPS interface for management of the device. If any of the above interfaces need to be enabled, it should be ensured that the device is installed in a network that is only accessible by authorized personnel.

6.5.2 Create a Backup of Device-Specific Data

When the device configuration is complete:

- Consider creating a backup copy of the configuration. For example, place the backup file in a device-specific folder that is only accessible by authorized personnel.
- Include other device-specific data. For example, copy device-specific private keys or certificates to the same device-specific folder.
- Keep the backup files separate from the device in a secure location.

This minimizes effort to replace a device should the hardware become inoperable.

6.6 Possible Hardware Modifications for Security

The following descriptions apply to:

- The possible hardware modifications for a device out-of-the-box.
- Possible hardware modifications as part of operation or maintenance.

Perform the following hardware modification steps, like covering or obstructing a slot or a port, as needed:

- Restrict physical (visual) access to the device and port LEDs.

6.6.1 Restrict Physical (Visual) Access to the Device and Port LEDs

For high security requirements, perform the following steps as needed:

- Install the device in a cabinet with an opaque door.
- Cover or obstruct the LEDs with a removable cover.

6.7 Device Installation

The following description applies to:

- The installation of a device in a new system.
- Changes to the device as part of operation or maintenance.

For more information about device installation, please see *Appendix A - Radio Hardware*.

6.8 Operation

In the operation phase of the device, it is assumed the appropriate physical and logical steps to set up the device and operate properly regarding the functional and security aspects of the device are observed. This reduces the required security steps during the operation phase to the considerations already described in this document.

6.8.1 Environmental Conditions

Obey the environmental conditions given in *Appendix F - Detailed Radio Specifications*. Do not open the device.

6.8.2 Connectivity

Obey instructions for connecting the Ethernet port.

6.9 Maintenance

6.9.1 Software Update

If necessary, perform a software update:

- For the security aspects.
- For detailed steps, see the *IH Browser User Manual* at www.prosoft-technology.com.

6.9.2 Hardware Replacement

Note: Do not open the device.

Perform the following steps:

- Perform an initial software update.
- Perform the software configuration, for example, by transferring the existing configuration of the old device to the new device.

6.9.3 Hardware Repair

Should the device need repair, consider the following recommendations:

- Do not open the device.
- Send the device to the manufacturer for repair.
- Keep a backup copy of the device configuration.

If necessary and possible, reset the device to factory defaults to erase the configuration and other confidential data before returning to the manufacturer.

6.10 Decommissioning

For high security requirements, consider physical destruction. Secure physical destruction addresses the possible reading-out of memory blocks from the flash memory and makes deletion and wiping redundant.

Note: If the device is to be used in the future, consider leaving the device and its software intact and deleting or wiping only the data on the device and on the external memory.

6.10.1 Destruction of Confidential Data

Note: Resetting the device to the default state performs normal file deletion operations on the device and the external memory which may leave some of the file contents or blocks in the flash memory intact.

If there are high security requirements, consider the physical destruction of the device and the external memory if used.

6.10.1.1 Reset to the Delivery State

- For the deletion of data, perform the following steps as needed:
- Reset the device to the factory default state. This deletes the configuration in the device.
- If necessary, manually delete the configuration profiles on the external memory and/or any other files on it.

6.10.2 Secure Physical Destruction of Device and Components

For the secure physical destruction of physical components, perform the following steps as needed:

- Physically destroy any external memory SD Card that was used with the device. This addresses:
  - Any configuration file on the external memory.
- Physically destroy the device, including the flash memory chips. This addresses:
  - The HTTPS certificate in the device.
  - The configuration in the device.
  - Any other files in the device.

7 Initial Access - Cybersecurity

A small set of services are activated in the factory default state as they may be required for initial configuration. For cybersecurity reasons, the remaining services are disabled and can only be activated via web interface setting changes. The following table provides an overview.

Service	Port Number	Accessibility	Authenticated	Encrypted
Aeroscout	1144	Disabled	-	-
DHCPv4 client	67	Enabled	-	-
DNS client	546	Disabled	-	-
Ethernet IP Agent (RO)	44818, 502, 2222	Disabled		
FTP server	20, 21	Disabled	-	-
HTTP	80	Re-direct to port 443 only	-	-
HTTPS	443	Enabled	Yes	Yes
IH Browser	800	Enabled	-	-
Ping	ICMP	Enabled		-
PTP Filter	319, 320	Disabled		-
SNMPv1/v2c	161, 162	Disabled	-	-
SNTP	123	Disabled	-	-
Syslog	514	Disabled	-	-
Radius Client	1812	Disabled	Yes	Yes
Telnet	23	Disabled	-	-
Interface	**Mode**	**Accessibility**	**Authenticated**	**Encrypted**
Ethernet	Promiscuous	Enabled	-	-
RS-232C (RLX2 only)	Proprietary serial log (no console access)	Enabled	-	-
WiFi - In factory default	Inactive	Disabled	-	-
WiFI - After password and passphrase are set	Active	Enabled	Yes	Yes

7.1 DHCPv4 Client

If the device's Ethernet is connected to a network that has a DHCP Server, the device can automatically obtain its IP Address. This will allow the initial configuration of the device to proceed without assigning a temporary IP Address.

7.2 IH Browser

The device's IH Browser service participates in discovery of the device. Once discovered, the IH Browser can be used to assign a temporary IP Address to the device if there is no DHCP Server present. Once the temporary IP Address is assigned the device's web interface can be accessed to set a new password and passphrase to activate the wireless interface.

The IH Browser displays information about the device. The IH Browser can also be used to extract a device's configuration or update the device's firmware or configuration, however it uses the device's HTTPS interface to do so which is secure. No private security data is transferred to/from the IH Browser on its port 800 interface.

8 Appendix A - Radio Hardware

8.1 Radio Power Requirements

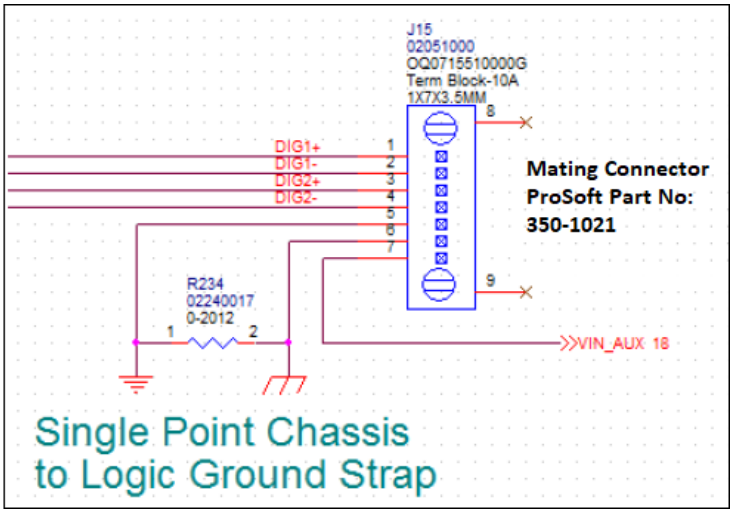
The ELXM-SW6 accepts voltages between 10 and 30 VDC, with an average power draw of less than 6 Watts. A detachable power connector (ProSoft Technology part number 350-1021) comes with the ELXM-SW6, as shown below. The connector terminal power pins are labeled on the front panel overlay as DC+ DC- and 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 schematic below.

1) Ethernet and serial port RJ45 connector metal shields
2) Micro-SD and SIM socket metal shields
3) Pushbutton switch metal shield
4) All CPU heat sink and board mounting holes
5) Input power connector



- The ELXM-SW6 shall be installed by trained personnel only, as outlined in the installation instructions.

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.

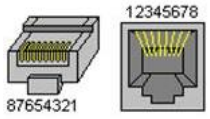
8.2 Ethernet Cable Specifications

- 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 module 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 module detects the cable type and uses the appropriate pins to send and receive Ethernet signals.

8.3 Ethernet Cable Configuration

8.3.1 Ethernet Cable Configuration

A diagram of the ELXM-SW6 pin assignments are shown below.



8.3.1.1.1 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-

8.3.1.1.2 Crossover Cable

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

9 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).

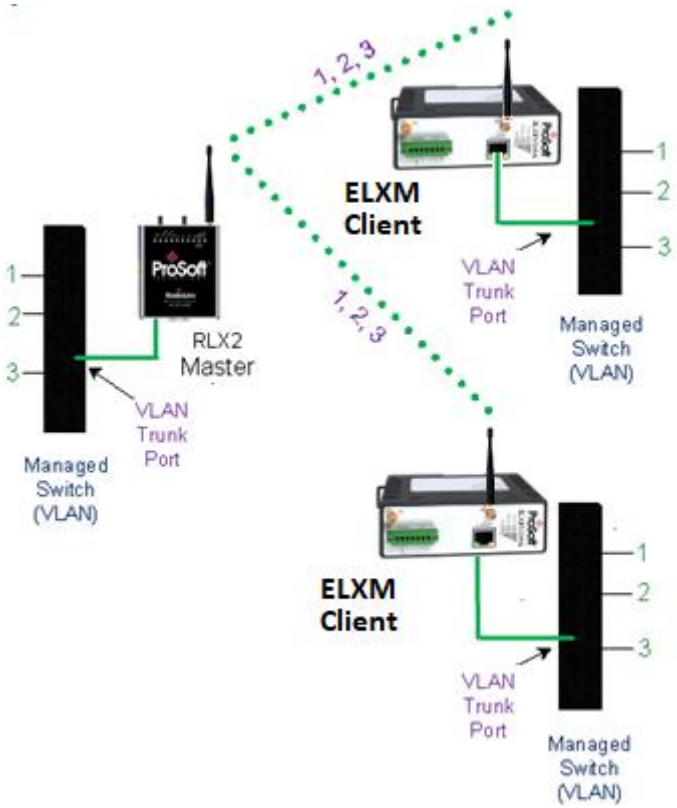
Constraining data to a particular Virtual LAN requires that the ELXM-SW6 tags packets with a VLAN identifier. VLAN tagging simply adds extra information to the packet header of Ethernet frames, so VLAN-enabled switches know how to pass along the data.

The ELXM-SW6 (version 33 and later) provides:

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

9.1 Transparent Support of VLAN Tags (802.1Q)

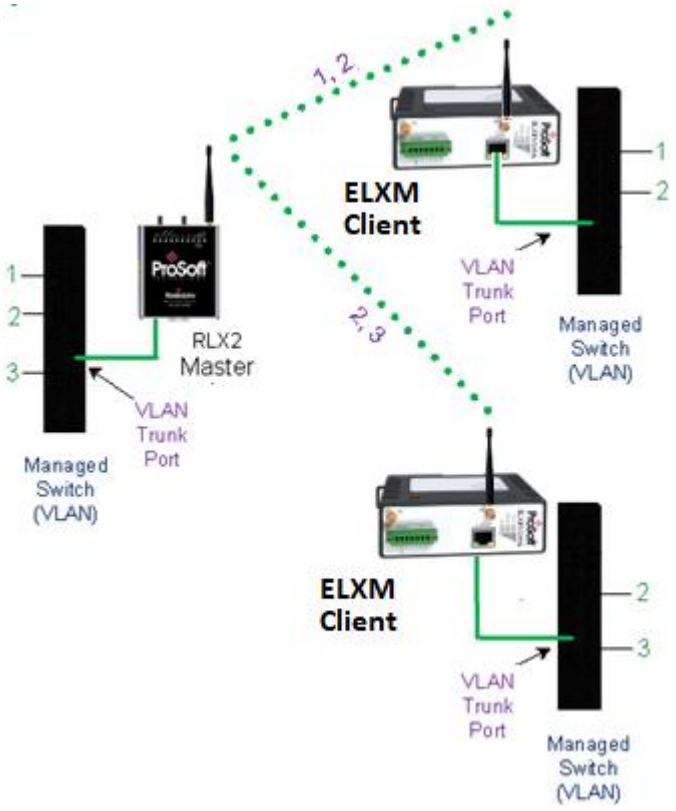
The following provides an example of transparent communication between Managed switches using VLAN trunking. This is achieved by default by the ELXM-SW6s without any VLAN configuration necessary.



9.2 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 ELXM-SW6 supporting the Managed Switch passes on the 802.1Q frames. This example shows support for ELXM-SW6 to ELXM-SW6 VLANs using one or more Trunk Links and is achieved with specific configuration of the ELXM-SW6's VLAN settings.

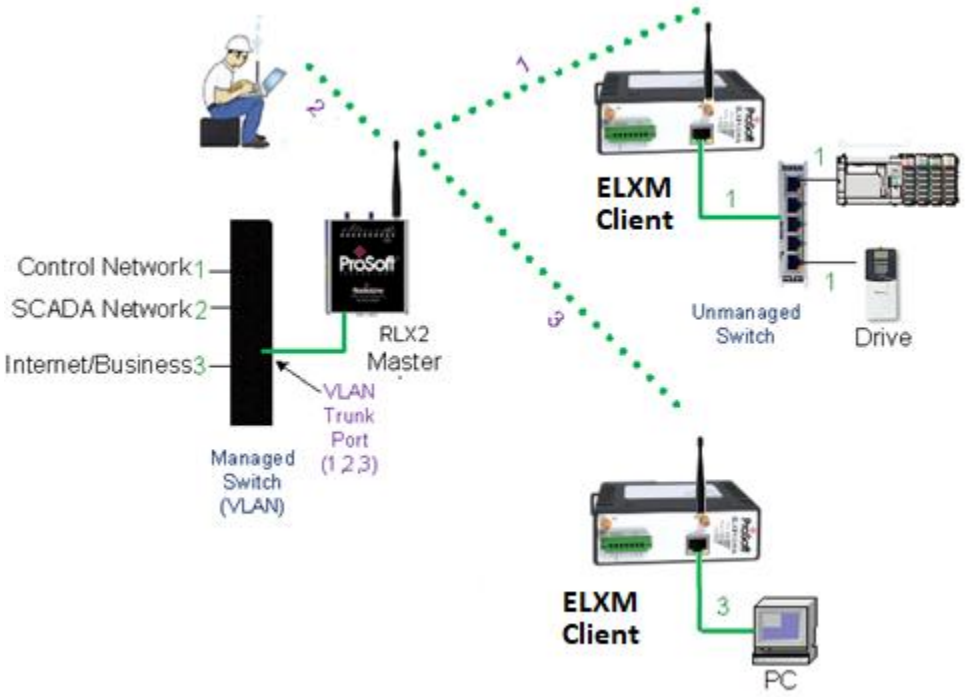
- The 1st remote managed switch only gets VLAN 1 and 2 traffic.
- The 2nd remote managed switch only gets VLAN 2 and 3 traffic.



9.3 Port/Radio-based VLAN Tagging without Managed Switches

In this example, the network has three VLANs (capacity for 15). Each VLAN has access to a specific ELXM-SW6 port. The ELXM-SW6 supporting the Managed Switch passes on the 802.1Q frames. The wireless network also supports ELXM-SW6 to ELXM-SW6 VLANs using one or more Trunk Links.

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



10 Appendix C - EtherNet/IP and Modbus TCP/IP Support

Diagnostic and status information is obtained from the ELXM-SW6 by using the EtherNet/IP or Modbus TCP/IP protocols.

10.1 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.

10.1.1 Modbus Memory Map Diagnostic Information

The following table lists the Modbus register addresses to read the ELXM-SW6 diagnostic and status information. Use Modbus Function Code 4 (Read Input Registers(3X)).

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 in firmware *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

10.2 EtherNet/IP™ Server Support

The following are the CIP™ object definitions to read the ELXM-SW6 Radio diagnostic and status information.

10.2.1 ELXM-SW6 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

10.2.2 ELXM-SW6 Information Extended

Class ID: 0xA2 (162)
Number of Instances: 1
Available on ELXM-SW6s with firmware *ELXM-SW6_v0038_R* or greater.

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

10.2.3 File CRC Signatures

Class ID: 0xA3 (163)
Number of Instances: 1
Available on ELXM-SW6s with firmware *ELXM-SW6_v0038_R* or greater.

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

11 Appendix D - AP Channel-Frequency Table

The following table displays the available channels/frequencies in the ELXM-SW6 when in AP mode. Note that ELXM-SW6s configured for FCC and ETSI regulatory domains do not have the same available channels. Also, some channels may have usage or power restrictions (for example, indoor or outdoor) in some locations. Highlighted 6 GHz channels in blue color denote a “PSC” channel. The ELXM-SW6 will only scan on PSC channels while looking for APs.

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	✓	Short Range Device
153	5765	✓	Short Range Device
157	5785	✓	Short Range Device
161	5805	✓	Short Range Device
165	5825	✓	Short Range Device
1	5955	Only Client modes†	Only Client modes†
5	5975	Only Client modes*	Only Client modes*
9	5995	Only Client modes†	Only Client modes†
13	6015	Only Client modes†	Only Client modes†
17	6035	Only Client modes†	Only Client modes†

21	6055	Only Client modes*	Only Client modes*
25	6075	Only Client modes†	Only Client modes†
29	6095	Only Client modes†	Only Client modes†
33	6115	Only Client modes†	Only Client modes†
37	6135	Only Client modes*	Only Client modes*
41	6155	Only Client modes†	Only Client modes†
45	6175	Only Client modes†	Only Client modes†
49	6195	Only Client modes†	Only Client modes†
53	6215	Only Client modes*	Only Client modes*
57	6235	Only Client modes†	Only Client modes†
61	6255	Only Client modes†	Only Client modes†
65	6275	Only Client modes†	Only Client modes†
69	6295	Only Client modes*	Only Client modes*
73	6315	Only Client modes†	Only Client modes†
77	6335	Only Client modes†	Only Client modes†
81	6355	Only Client modes†	Only Client modes†
85	6375	Only Client modes*	Only Client modes*
89	6395	Only Client modes†	Only Client modes†
93	6415	Only Client modes†	Only Client modes†
97	6435	Only Client modes†	
101	6455	Only Client modes*	
105	6475	Only Client modes†	
109	6495	Only Client modes†	
113	6515	Only Client modes†	
117	6535	Only Client modes*	
121	6555	Only Client modes†	
125	6575	Only Client modes†	
129	6595	Only Client modes†	
133	6615	Only Client modes*	
137	6635	Only Client modes†	
141	6655	Only Client modes†	
145	6675	Only Client modes†	
149	6695	Only Client modes*	
153	6715	Only Client modes†	
157	6735	Only Client modes†	
161	6755	Only Client modes†	
165	6775	Only Client modes*	
169	6795	Only Client modes†	
173	6815	Only Client modes†	
177	6835	Only Client modes†	
181	6855	Only Client modes*	
185	6875	Only Client modes†	
189	6895	Only Client modes†	
193	6915	Only Client modes†	
197	6935	Only Client modes*	
201	6955	Only Client modes†	
205	6975	Only Client modes†	
209	6995	Only Client modes†	
213	7015	Only Client modes*	
217	7035	Only Client modes†	
221	7055	Only Client modes†	
225	7075	Only Client modes†	
229	7095	Only Client modes*	
233	7115		

* Preferred Scanning Channel (PSC)

† Only used when bonded with a PSC channel

12 Appendix E - Emission Regulations

This chapter contains the maximum emissions allowed by the FCC in the United States and ETSI in Europe. This data should only be considered guidelines. Consult official FCC or ETSI documents for the latest official regulations.

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

12.1 2.4 GHz Band, FCC, 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

12.2 2.4 GHz Band, FCC, 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 radio's transmitter output, the antenna gain may be increased by 3 dB.

12.3 5 GHz Band, FCC, 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

12.4 5 GHz Band, FCC, 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

12.5 6 GHz Band, FCC

6 GHz Band	Frequency Range (GHz)	Channels	Permitted Location	Maximum EIRP		Maximum Power Spectral Density EIRP
				dBm	mW	dBm/MHz
UNII-5	5.925 to 6.425	1-93	Indoor	24	250	-1
UNII-6	6.425 to 6.525	97-113	Indoor	24	250	-1
UNII-7	6.525 to 6.885	117-185	Indoor	24	250	-1
UNII-8	6.885 to 7.125	189-233	Indoor	24	250	-1

12.6 2.4 GHz Band, ETSI

Frequency Range (GHz)	Channels	Permitted Location	Maximum EIRP		Maximum Power Spectral Density EIRP
			dBm	mW	dBm/MHz
2.400 to 2.4835	1-13	Indoor or Outdoor	20	100	10

12.7 5 GHz Band, ETSI

5 GHz Band	Frequency Range (GHz)	Channels	Permitted Location	Maximum EIRP		Maximum Power Spectral Density EIRP
				dBm	mW	dBm/MHz
Sub-band 1	5.150 to 5.250	36, 40, 44, 48	Indoor	23	200	10
Sub-band 2	5.250 to 5.350	52, 56, 60, 64	Indoor	23*	200*	10*
Sub-band 3	5.470 to 5.725	100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140	Indoor or Outdoor	30*	1000*	17*
SRD band	5.725 to 5.875	149, 153, 157, 161, 165, 169, 173	Indoor or Outdoor	14	25	NA

*If TPC is not used, limits are 3dB lower for both EIRP and PSD EIRP.

12.8 6 GHz Band, ETSI

6 GHz Band	Frequency Range (GHz)	Channels	Permitted Location	Maximum PEIRP		Maximum Power Spectral Density EIRP
				dBm	mW	dBm/MHz
UNII-5	5.925 to 6.425	1-93	Indoor	23	200	10

13 Appendix F - Detailed Radio Specifications

13.1 ELXM-SW6 Detailed Specifications

13.1.1 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) 5.975 GHz to 7.095 GHz (FCC/ETSI)* * Client modes only	36 to 48 52 to 64* 100 to 140* 149 to 165 149 to 165 5 to 229 (PSC channels only)*
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 - 5 GHz / 6 GHz) 17 dBm @ MCS0, (802.11ax/gn - 2.4 GHz) 10 dBm @ MCS11, (802.11ax - 5 GHz / 6 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	

20 MHz Channels	40 MHz Channels	80 MHz Channels	Rate	Streams
8.6 Mbps	17.2 Mbps	36.0 Mbps	MCS0	1 Stream
143.3Mbps	286.8 Mbps	600.5 Mbps	MCS11	
17.2 Mbps	34.4 Mbps	73.1 Mbps	MCS0	2 Streams
286.8 Mbps	573.5 Mbps	1201.0 Mbps	MCS11	

Receiver Sensitivity (Typical, 1x1 chain)	-95 dBm @ MCS0, (802.11ax - 5 GHz / 6 GHz) -92 dBm @ MCS0, (802.11ax - 2.4 GHz) -77 dBm @ MCS7, (802.11ax - 5 GHz / 6 GHz) -72 dBm @ MCS7, (802.11ax - 2.4 GHz) -66 dBm @ MCS11, (802.11ax - 5 GHz / 6 GHz) -63 dBm @ MCS11, (802.11ax - 2.4 GHz)
Security	WPA2 Personal/Enterprise – 802.11i AES Legacy WPA support

13.1.2 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, 5.11 x 1.57 x 3.94 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)

13.1.3 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

13.1.4 Agency Approvals & Certifications

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

14 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	Like 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 Radio products 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.
Bandwidth	see *Throughput*
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	*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. For example: A modem

Term	Description
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	*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, like 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 can operate in two frequency bands. On a wireless network, dual-band devices can operate 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.

Term	Description
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 is 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.

Term	Description
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 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 with it.
Point-to-Point	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 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	An ELXM-SW6 Radio in *Repeater* mode can only connect to other ProSoft 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.

Term	Description
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 that is 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 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.

15 Support, Service, and Warranty

15.1 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.orders@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 see:
www.prosoft-technology.com/About-Us/Contact-Us

15.2 Warranty Information

For 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/Services-Support/Return-Material-Instructions