



AirLink MG90

Software Configuration Guide

Important Notice

Information relating to this product and the application or design described herein is believed to be reliable, however such information is provided as a guide only and Semtech assumes no liability for any errors in this document, or for the application or design described herein.

Semtech reserves the right to make changes to the product or this document at any time without notice. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. Semtech warrants performance of its products to the specifications applicable at the time of sale, and all sales are made in accordance with Semtech's standard terms and conditions of sale.

SEMTECH PRODUCTS ARE NOT DESIGNED, INTENDED, AUTHORIZED OR WARRANTED TO BE SUITABLE FOR USE IN LIFE-SUPPORT APPLICATIONS, DEVICES OR SYSTEMS, OR IN NUCLEAR APPLICATIONS IN WHICH THE FAILURE COULD BE REASONABLY EXPECTED TO RESULT IN PERSONAL INJURY, LOSS OF LIFE OR SEVERE PROPERTY OR ENVIRONMENTAL DAMAGE. INCLUSION OF SEMTECH PRODUCTS IN SUCH APPLICATIONS IS UNDERSTOOD TO BE UNDERTAKEN SOLELY AT THE CUSTOMER'S OWN RISK. Should a customer purchase or use Semtech products for any such unauthorized application, the customer shall indemnify and hold Semtech and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs damages and attorney fees which could arise.

The Semtech name and logo are registered trademarks of the Semtech Corporation. All other trademarks and trade names mentioned may be marks and names of Semtech or their respective companies. Semtech reserves the right to make changes to, or discontinue any products described in this document without further notice. Semtech makes no warranty, representation or guarantee, express or implied, regarding the suitability of its products for any particular purpose. All rights reserved.

Wireless Communications

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. The Semtech product should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Semtech accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Semtech product, or for failure of the Semtech product to transmit or receive such data.

Warranty

%AirLink Products only%Warranty information for AirLink products is available at www.sierrawireless.com/end-user-warranty.

Safety

Do not operate the Semtech product in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or near any equipment which may be susceptible to any form of radio interference. In such areas, the Semtech product should be powered off.

Qualcomm licenses

%MODULES ONLY% Semtech's cellular modules are sold subject to certain notices and restrictions regarding patent licenses from Qualcomm Incorporated. These notices and restrictions are available at www.sierrawireless.com/qualcomm-notices.

Sierra Wireless

Semtech Corporation acquired Sierra Wireless in January 2023. The Sierra Wireless brand is gradually being phased out. During the phase-out period, references to both "Semtech" and "Sierra Wireless" may appear in product documentation.

Contact Information

Sales information and technical support, including warranty and returns	Web: sierrawireless.com/company/contact-us/ Global toll-free number: 1-877-687-7795 6:00 am to 5:00 pm PST
Corporate and product information	Web: sierrawireless.com

Revision History

Revision number	Release date	Changes
1	October 2016	Document created
2	January 2017	MC74xx used to identify radio module series, replacing MC7455 Clarified AMM statement in Configuring an MG90 Router Added GPS fields to new section NMEA Messaging 'Additional Options' Added fields to Table A-2, Cellular Info section (MEID, Band Number, Bandwidth, RSRP, RSRQ, SINR, Hardware Version, Roaming Indicator, Service, Provision Status) Added Advanced modem Initialization example for private network link in Cellular WAN Link Configuration and Table E-3 Updated Configuring VPN Profiles (reboot requirement for VPN updates)
3	July 2017	Added new radio modules — MC7354, Bandrich M535
4	November 2017	Noted Bluetooth adapter default configuration in Devices > Bluetooth. Added LED chase sequence for firmware updates in Table K-1.

Revision number	Release date	Changes
5	June 2018	Added Advanced Configuration Login Added GPS Forwarding Threshold options Added PPPoE WAN support for USB-to-Ethernet adapter Added note indicating IKEv2 VPNs only, when MOBIKE is used Added note concerning module firmware update when device has two different Sierra Wireless modules Support for multiple Host-to-LAN simultaneous VPN servers Added LCI options for private DNS zones Added GPIO and GPIO Status applications Added EM75XX module support Added Status Broadcast option Updated Cellular WAN Link Configuration MTU Size fields Added Enable/disable option to LAN Access Points configuration Added IGMP Snooping enable/disable to LAN Segment Configuration Added GPS Dead Reckoning configuration and updated GNSS LED behavior Removed option to enable/disable automatic purging of unused firmware images Added FirstNet SIM support for use with EM7565 modules Added DSCP option to QoS Priority Rules Added option to switch MG90 from non-FIPS to FIPS (one way only) Updated Management Tunnel Configuration (added UDP ports, replaced selectable monitors with Tunnel Automatic Monitor)
6	August 2018	Added Purge on Next Boot field for purging firmware images Noted Split Access security consideration Added 'Automatic' option for Gateway Virtual IP assignment
7	December 2019	Updated Introduction (Terminology, Performance Tips) Updated Viewing Only Configuration Settings (Easy Access) Added GNX AirLink Companion Device support (Configuring the Serial Port, Add/Configure LAN Segments, Configuring the Serial LAN Segment, Connecting to GNX AirLink Companion Device, GNX Companion application) Updated Multi-VPN Support (allow single tunnel with failover; added Connection Method to WAN link configuration screens) Updated Broadcast Router Status Updated Configuration Settings: Backup, Restore, and Reset Updated GPS Configuration Set Up (new layout, added Enable Jitter Filter, added turn-based forwarding, added Report Fixed Direction When Stationary) Updated Updating the System (new layout, added radio module firmware management features) Added Policy Based Routing Rules Updated Device Service Configuration screen (added NTP Server options) Added Certification Configuration

Revision number	Release date	Changes
8	January 2021	Updated for MGOS 4.3.1: ▪ Updated Accessing the Local Configuration Interface (LCI), Viewing Only Configuration Settings (Easy Access) ▪ Removed Advanced Configuration Login ▪ Updated Configuring User Access (username / password requirements) ▪ Updated Broadcast Router Status (new fields) ▪ Added Private Network (including CBRS) Configuration support ▪ Updated Gateway State Beacon ▪ Updated Setting up GPS connectivity (message note) ▪ Updated Storing Radio Module Firmware in MG90 (loading signed images) ▪ Changed chapter numbers (15 and up) to appendix letters) ▪ Updated Extended status screen (added SCC data) ▪ Updated Status Broadcast (new screen fields) ▪ Added Security > Settings ▪ Updated LAN Segment Configuration (LAN > LAN Segments > Configure) (added SSH access option) ▪ Updated General > Tools (removed toggleband) ▪ Updated JSON Data (schema and example)
9	March 2021	▪ Standardized MGOS/MG90 references to LCI as "MGOS" ▪ Added MG90 5G references ▪ Added EM9190 module references ▪ Updated WAN Link Status (Extended) screen/fields to include MG90 5G data ▪ Updated Status Broadcast Configuration screen/fields to include MG90 5G data ▪ Updated Cellular WAN Link Configuration screen/fields to include MG90 5G data
10	March 2022	▪ Removed 6.1.1.1 Private Network (and CBRS) Configuration
11	May 2022	▪ Updated Status Broadcast Configuration to report individual VPN statuses (VPN Status option) ▪ Added AMM-Initiated Multiple Unit Reboot support ▪ Added Private Network Configuration ▪ Added TCP MSS Clamping support ▪ Updated Cellular WAN Link Configuration • Updated fields: Setting for Band, MTU Size field, Network Type (added note) • Added field: Enable TCP MSS Clamping • Removed 5G module restrictions from fields: Allow Blank APN, Setting for Band, Custom Band Setting Mode, ▪ Updated Signal Strength Policy to include additional metrics ▪ Updated JSON Data (added new wanState and vpnState values)

Revision number	Release date	Changes
12	November 2022	▪ Added certificate Key Algorithm usage notes (Configuring VPN Profiles, LCI-initiated — Secure method, Table C-5) ▪ Added field (Single Subnet Per Child SA) to configure VPN for connection to Cisco ASA (Table E-16) ▪ Added DNS logging fields (Table G-3) ▪ Updated document template
13	August 2025	▪ Retitled and updated 14.2 Downloading and Installing Auto Software Updates (reworded Downloading Auto Software Updates section; added Disable Boot Checks on Ignition Shutdown note) ▪ Updated Table E-16, WAN > VPNs > Add New VPN (or Configure) screen fields (clarified Allow Management Tunnel Bypass usage) ▪ Updated Table G-8, General > Auto Software Updates screen fields (added Disable Boot Checks on Ignition Shutdown) ▪ Replaced MC74XX references with MC7430/MC7455; replaced EM75XX references with EM7511/EM7565

Contents

Important Notice	2
Wireless Communications	2
Warranty	2
Safety	2
Qualcomm licenses	3
Sierra Wireless	3
Contact Information	3
Revision History	3
Introduction	14
1.1 Overview	14
1.2 About This Document	14
1.3 FIPS vs. Non-FIPS	15
1.4 Performance Tips	15
1.5 Terminology	15
1.5.1 Module Types	15
1.6 Tools and Reference Documents	16
Router Access and Configuration	17
2.1 Configuring an MG90 Router	17
2.2 Accessing the Local Configuration Interface (LCI)	17
2.3 Navigating the LCI Tabs and Screens	18
2.4 Viewing Only Configuration Settings (Easy Access)	19
Configuring Startup/Shutdown Behavior	21
3.1 Startup Behavior	21
3.2 Shutdown Behavior	21
Preparing the Network Interfaces	23
4.1 Configuring Cellular Devices	23
4.2 Configuring Ethernet Ports	24
4.3 Configuring Wi-Fi Devices	24
4.4 Configuring a Serial Modem Device	25
4.5 Configuring the Serial Port	25
4.6 Configuring the Bluetooth Device	26
Administration	27
5.1 Displaying General Information	27

5.2 Obtaining WAN Status Details	27
5.3 Broadcast Router Status	28
5.4 Configuring User Access	30
5.5 Changing the Root Password	32
5.6 Configuring Supported LCI Access Protocols	32
5.7 Backing Up, Restoring, and Factory Resetting the Router	33
5.7.1 Backing up the current configuration	34
5.7.2 Restoring an earlier configuration	34
5.7.3 Factory resetting the configuration	35
5.7.4 AMM-Initiated Multiple Unit Reboot	35
5.8 Configuring Services	36
5.8.1 Configuring Event Reporting	36
5.8.2 Enabling the Legacy Beacon Service	36
5.8.3 Configuring Wi-Fi Country Code	37
5.8.4 Configuring NTP Servers	37
5.9 Using Diagnostic Tools	37
5.10 Running Custom Scripts	38
Setting Up The WAN	39
6.1 Basic WAN Link Configuration	39
6.1.1 Cellular WAN Link Configuration	40
6.1.1.1 Private Network Configuration	42
6.1.2 Wi-Fi WAN Link Configuration	43
6.1.3 Ethernet WAN Link Configuration	43
6.1.3.1 Setting up PPPoE WAN	44
6.1.4 Serial WAN Link Configuration	45
6.2 Defining an Access Point Profile for Wi-Fi Links	46
6.3 Using Pilot Ping to Pre-test WAN Links	48
6.4 Using WAN Monitors to Detect Lost Connections	49
6.5 Setting up WAN Link Policies	51
6.5.1 Special Considerations for Wi-Fi Links	53
6.5.2 Dynamic Priority Policy Overview	53
6.5.2.1 Dynamic Priority Policy Example	54
6.5.3 Geographical Regions Policy Overview	55
6.5.3.1 Geographical Regions Policy Example	56
6.5.4 Time Period Policy Overview	57
6.5.5 Velocity Policy Overview	57
6.5.6 Signal Strength Policy Overview	58
6.5.6.1 Signal Strength Policy Examples	59
6.5.7 Use Cases	60
6.5.7.1 Dynamic Priority Policy and Velocity Policy Combination	60
6.6 Setting up the WAN Firewall	62
6.6.1 Configuring WAN Networking Rule Firewall Settings	62
6.6.1.1 Defining WAN Firewall Rules	62

6.6.1.2 Deleting WAN Firewall Rules	62
6.7 WAN Link Recovery	63
Setting up the LAN	64
7.1 Ethernet LAN Link Configuration	64
7.2 LAN Access Point Configuration	65
7.3 Configuring LAN Segments	65
7.3.1 Add/Configure LAN Segments	65
7.3.2 Assign a Device to a Different LAN Segment	67
7.3.3 Delete a LAN Segment	67
7.4 Configuring DHCP and Static IP Addresses	68
7.5 Configuring the Serial LAN Segment	68
7.6 Setting up the LAN Firewall	69
7.6.1 Configuring LAN Networking Rule Firewall Settings	69
7.6.2 Defining LAN Firewall Rules	69
7.6.3 Deleting LAN Firewall Rules	69
7.7 Setting up Virtual LANs	69
7.8 Setting up Captive Portals	70
Supporting Connection From GNX AirLink Companion Device	72
Performance Tuning	74
9.1 Configuring Load Balancing	74
9.2 Setting Quality of Service (QoS)	75
9.2.1 Defining QoS Policies	75
9.3 Configuring LAN Throughput Reporting Frequency	76
How to configure a VPN	77
10.1 Details Required to Configure VPNs	77
10.2 Configuring VPN Profiles	77
10.3 Setting Up Dead Peer Detection (DPD)	79
10.4 Multi-VPN Support	79
10.4.1 Configure WAN Links for Multi-VPN	80
10.4.2 View Assigned VPNs	81
10.5 Configuring DNS Zones for Private DNS Server Use	82
10.5.1 LCI WAN Link Private Zone Configuration	82
10.5.2 Manual Private Zone Configuration	83
Certificate Configuration	85
11.1 Certificate Profile Management	85
11.1.1 Certificate Enrollment Methods	86
11.1.1.1 LCI-initiated — Secure method	86

11.1.1.2 LCI-initiated — Legacy method	88
11.1.1.3 AMM-initiated — Secure method	89
11.1.2 Renewing a Certificate	89
11.1.3 Deleting a Certificate Profile	90
11.2 Using a Certificate Profile	90
11.2.1 Creating a combined CA certificate	92
Setting up GPS connectivity	94
12.1 GPS Configuration Set Up	95
12.2 Configuring Dead Reckoning	97
12.3 Configuring Turn-based Forwarding and Reporting	98
Applications	100
Updating the System	101
14.1 Configuring Auto Software Updates	101
14.2 Downloading and Installing Auto Software Updates	103
14.3 Forcing an OTA Update	104
14.4 Radio Module Firmware Images	104
14.4.1 Firmware Overview	104
14.4.2 Storing Radio Module Firmware in MG90	105
14.4.2.1 Loading an image from AMM	106
14.4.2.2 Loading a signed image from Computer	106
14.4.3 Automatic Firmware Upgrades	108
14.4.4 Firmware Image Switching	109
14.4.4.1 SIM-based Carrier Switching	109
14.4.4.2 Manual Firmware Switching (Forcing a Switch)	110
14.4.4.3 Image Switching Process	110
14.4.5 Purging Firmware Images	112
14.4.6 Listing Firmware Images	112
Status Tab	114
A.1 WAN Link Status Tab	114
A.1.1 Summary status screen	114
A.1.2 Extended status screen	115
A.2 General Information	120
A.3 Status Broadcast	123
Devices Tab	126
B.1 Devices > Cellular	126
B.2 Devices > Ethernet	127
B.3 Devices > Wi-Fi	128

B.4 Devices > Serial Modem	129
B.5 Devices > Serial	130
B.6 Devices > Bluetooth	131
B.6.1 Bluetooth Adapter Configuration (Devices > Bluetooth > Configure)	131
Security Tab	133
C.1 Security > Users	133
C.2 Security > Change Root Password	134
C.3 Security > Certificate Management	135
C.3.1 Existing Certificate/Key Upload Screen	136
C.3.2 CSR Configuration Screen	137
C.3.3 Certificate Signing Request Summary Screen	139
C.3.4 Signed Certificate Upload Screen	139
C.4 Security > Settings	140
LAN Tab	141
D.1 LAN > Ethernet Links	141
D.1.1 LAN Ethernet Configuration (LAN > Ethernet Links > Configure)	141
D.2 LAN > Access Points	144
D.2.1 Access Point Configuration (LAN > Access Points > Configure)	144
D.3 LAN > LAN Segments	153
D.3.1 LAN Segment Configuration (LAN > LAN Segments > Configure)	154
D.4 VLAN Configuration (LAN > Virtual LANs)	156
D.5 LAN > Networking Rules, and LAN > LAN Segments > Networking Rules	158
D.6 LAN > LAN Throughput	163
D.7 LAN > Captive Portal	164
D.8 LAN > Captive Portal > Configure	165
WAN Tab	169
E.1 WAN > Links	169
E.1.1 WAN Link Configuration (WAN > Links > Configure)	170
E.1.1.1 Ethernet WAN Link Configuration	171
E.1.1.2 Cellular WAN Link Configuration	176
E.1.1.3 Wi-Fi WAN Link Configuration	184
E.1.1.4 Serial (Modem) WAN Link Configuration	185
E.1.2 WAN Link Policy Configuration (WAN> Links > Policies)	190
E.1.2.1 WAN > Links > Policies > Configure	191
E.2 WAN > Monitors	199
E.2.1 WAN > Monitors > Configure	200
E.3 WAN > VPNs	201
E.3.1 WAN > VPNs > (Management Tunnel) > Configure	202
E.3.2 IPSec VPN Configuration (WAN > VPNs > Add New VPN, and WAN > VPNs > (IPSec VPN) > Configure)	204

E.4 WAN > WiFi Networks	210
E.4.1 WAN > WiFi Networks > Add New WiFi Network/Configure Network	211
E.5 WAN > Networking Rules	220
E.6 WAN > Recovery	228
E.7 WAN > SIM Configuration	229
 GPS Tab	 230
 General Tab	 238
G.1 General > Startup	238
G.2 General > Shutdown	239
G.3 General > Services	240
G.4 General > Tools	242
G.5 General > Backup/Restore	244
G.6 General > Advanced Routing Rules	245
G.6.1 General > Advanced Routing Rules > Add New Rule/Configure Rule	246
G.7 General > Auto Software Updates	247
 Logs Tab	 252
H.1 Logs > Current Logs	252
H.2 Logs > Archived Logs	252
 Applications Tab	 254
I.1 General Purpose I/O Configuration	254
I.1.1 Using GPIOs	255
I.1.1.1 Sample GPIO Rule Script	258
I.1.2 GPIO Status	258
I.2 Telemetry	259
I.2.1 GNX Companion	260
 Logout Tab	 262
 LEDs	 263
K.1 LED Behavior	263
 JSON Data	 265
L.1 Broadcast Router Status — JSON Schema	265
L.2 Broadcast Router Status — Example Data	267

References	269
M.1 Web Site Support	269
M.2 Reference Documents	269

1: Introduction

1.1 Overview

The MGOS Local Configuration Interface (LCI) is the browser-based configuration utility for MG90 Series routers, including:

- MG90 5G
- MG90 LTE-A Pro (Cat 12)
- MG90 LTE-A (Cat 6)
- MG90 LTE

Note: Throughout this document, 'MG90' refers to all MG90 Series routers.

You can use the LCI to:

- Log in and configure device parameters
- Adjust network settings
- Change security settings
- Update events reporting and control outputs

1.2 About This Document

This document describes how to configure various MGOS features, provides a full listing of interface parameters, and provides additional information for troubleshooting the MG90.

- Configuration tasks
 - [Router Access and Configuration](#) on page 17
 - [Performance Tuning](#) on page 74
 - [Configuring Startup/Shutdown Behavior](#) on page 21
 - [Preparing the Network Interfaces](#) on page 23
 - [Administration](#) on page 27
 - [Backing Up, Restoring, and Factory Resetting the Router](#) on page 33
 - [Setting Up The WAN](#) on page 39
 - [Setting up the LAN](#) on page 64
 - [How to configure a VPN](#) on page 77
 - [Certificate Profile Management](#) on page 85
 - [Setting up GPS connectivity](#) on page 94
 - [Applications](#) on page 100
 - [Updating the System](#) on page 101 (Software updates and radio module firmware management)
 - [Configuring NTP Servers](#) on page 37
 - [Status Broadcast](#) on page 123 — Broadcast router status information over UDP.
- LCI — Tab parameters
 - [Status Tab](#) on page 114
 - [Devices Tab](#) on page 126
 - [Security Tab](#) on page 133
 - [LAN Tab](#) on page 141
 - [WAN Tab](#) on page 169
 - [GPS Tab](#) on page 230

- [General Tab](#) on page 238
- [Logs Tab](#) on page 252
- [Applications Tab](#) on page 254
- [Logout Tab](#) on page 262
- Additional information
 - [LEDs](#) on page 263

1.3 FIPS vs. Non-FIPS

This document describes features and options for non-FIPS-enabled and FIPS-enabled MG90 routers.

Important: *MG90 routers cannot be 'cross-graded' (FIPS to non-FIPS, non-FIPS to FIPS) through the software interface. To convert an MG90, contact Sierra Wireless Support.*

1.4 Performance Tips

When configuring the router, consider the following tips to improve device performance:

- Auto Software Updates (General > Auto Software Updates)
 - Download on High Cost Link — Over-the-air (OTA) firmware updates require large file transfer. To avoid unexpected cellular data usage charges, configure cellular links as "High Cost Link". By default, OTA firmware update is turned off while connecting on High Cost Links. See [Configuring Auto Software Updates](#) on page 101.

Tip: *If some links are too expensive to use for firmware downloads, make sure that this option is disabled and that the links that should not be used are marked as high cost.*

- For tips on load balancing, quality of service, and load throughput reporting, see [Performance Tuning](#) on page 74.
- Turn detection — To ensure location reports are sent when the vehicle is turning, see [Configuring Turn-based Forwarding and Reporting](#) on page 98.

1.5 Terminology

1.5.1 Module Types

MG90 routers come with either one or two embedded radio (cellular) modules for connection to cellular networks. Routers with two radio modules support simultaneous connection to two cellular networks—each connection requires a dedicated radio module. These radio modules are referred to in the LCI as positions CA and CB and may be LTE modules (MC7354, MC7430/MC7455, EM7511/EM7565) or 5G modules (EM9190), depending on the MG90 model.

The MG90 also comes with two Wi-Fi modules. Typically, one can be used as an access point and the other can be used as a WAN connecting to access points.

Radio (cellular) module — Up to two radio modules (e.g. MC7354, MC7430/MC7455, EM7511/EM7565, EM9190). Up to two SIM cards can be inserted for each module (CA, CB). From left to right, the SIM card slots are:

- A1 — First cellular radio module (CA), first SIM

- A2 — First cellular radio module (CA), second SIM
- B1 — Second cellular radio module (CB), first SIM
- B2 — Second cellular radio module (CB), second SIM

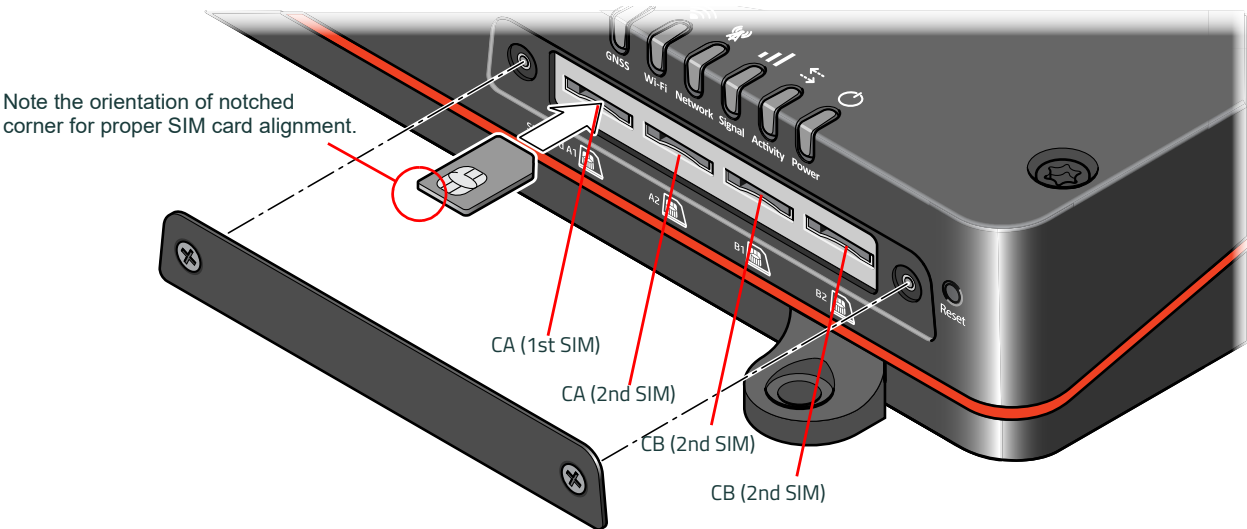


Figure 1-1: Installing the SIM Cards

Wi-Fi module — Two Wi-Fi modules, internal to the device.

- Wi-Fi A — Configured by default as Wi-Fi WAN. Used to connect to a local access point for data transfer.
- Wi-Fi B — Configured by default as Wi-Fi Access Point. Used to support connections to the router by wireless devices (up to 128 simultaneous connections).

1.6 Tools and Reference Documents

For MG90-related tools and documentation, go to <http://source.sierrawireless.com>.

Table 1-1: Related Documents

Document	Description
[1] AirLink MG90 Hardware User Guide	This document describes how to: ▪ Install the MG90 router hardware ▪ Connect the antennas ▪ Connect a notebook computer and other input/output (I/O) devices ▪ Interpret the router's LEDs

2: Router Access and Configuration

2.1 Configuring an MG90 Router

To configure an MG90 router, use either of the following methods:

- Use the browser-based LCI to directly configure the router (as described in this guide).
- If you have more than one MG90 router, use the AirLink Mobility Manager (AMM) application to copy (deploy) the configuration from one of your other routers to this router (refer to your AMM documentation for instructions).

Log in to AMM to monitor and manage your MG90 routers as described in the AirLink Mobility Manager Operation and Configuration Guide. If the MG90 does not appear in your AMM account dashboard, refer to your AMM documentation or contact Sierra Wireless Technical Support (see [Contact Information](#) on page 3).

Note: This document applies to AMM 2.17 and higher. AMM (AirLink Mobility Manager) is Sierra Wireless' cloud-based application.

2.2 Accessing the Local Configuration Interface (LCI)

Note: The LCI supports Internet Explorer 11 running on a Windows PC. Other browsers and devices may work but have not been certified by Sierra Wireless.

To access the LCI:

1. Insert the SIM card(s), if applicable. Refer to [1] AirLink MG90 Hardware User Guide (available from <https://source.sierrawireless.com>) for details.
2. Power on the MG90 router. The router should fully power up within two minutes.
3. Connect your computer to an Ethernet port 1–4. (These are configured by default as LAN connections.)
4. Launch your browser and connect to the LCI using one of the following addresses (and bypass any certificate notifications in the browser):
 - IP address: <https://172.22.0.1/MG-LCI/>
 - URL: <https://welcome.to.sierrawireless/MG-LCI/>

Note: By default, the MG90 uses HTTPS. If the router is configured to use HTTP and HTTPS, http can be used for the IP address and URL shown above.

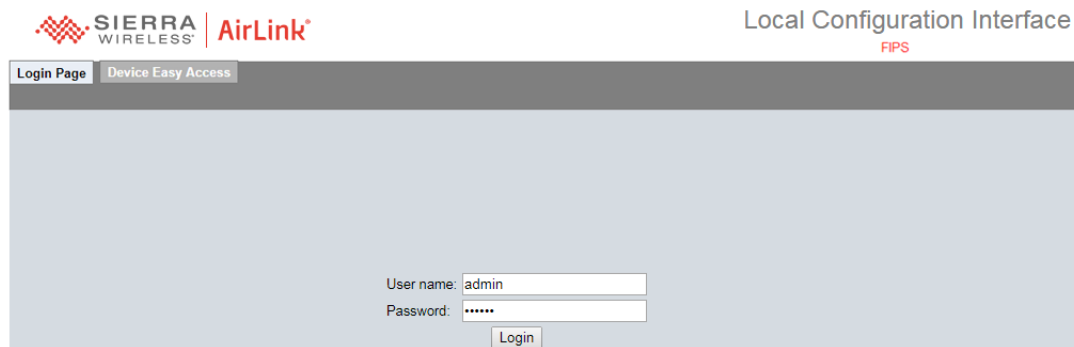


Figure 2-1: LCI Login Screen

Note: The red 'FIPS' indicator in the top-right portion of the screen appears only if the MG90 uses a FIPS-compliant encryption module.

5. Log in using the admin user credentials:

- User Name: admin
- Password:
 - MG90 router manufactured before February 2021 — admin (This is the default password)

Note: Make sure to change the admin password to prevent unauthorized access to the device. Otherwise, a warning dialog will appear, indicating that the user name and password must be different. See [Configuring User Access](#) on page 30 for instructions on [Updating Users](#).

- MG90 5G router, or MG90 router manufactured from February 2021 onward — Use the factory default password printed on the label attached to the bottom of the router.

Note: If there is no label on the bottom of the router, use 'admin' as the password.

The MG90 has two account types (see [Configuring User Access](#) on page 30 for details):

- admin — Used to directly access the LCI and update the MG90's configuration.
- user — Used to access the LCI to show the current status.

2.3 Navigating the LCI Tabs and Screens

The following are some basic tips for navigating in the LCI and updating the MG90's configuration:

- Most configuration changes take effect as soon as they are saved. If a change requires a router reboot (such as a change to the serial port), a message will appear.
 - Screens with a Save or Submit button — Click the button to save any changes made on the current screen.
 - You cannot 'undo' a change that has been saved.
 - Changes that have not been saved are automatically canceled if you:
 - Click the Cancel button (if available)
 - Change to a different tab
 - Use the browser options to go forward or backward
 - Refresh browser window to return to the WAN Status screen.

- Browser options:
 - Forward / Back icons (and keyboard shortcuts) — Regular browser functionality. Use these to move forward and backward through your history. Note that this cancels any changes in progress.
 - Refresh icon (and keyboard shortcut — for example, F5 for IE and Chrome) — Cancels any changes in progress and returns to the WAN Status screen.
- Log out — To log out of the LCI, click the Logout tab.

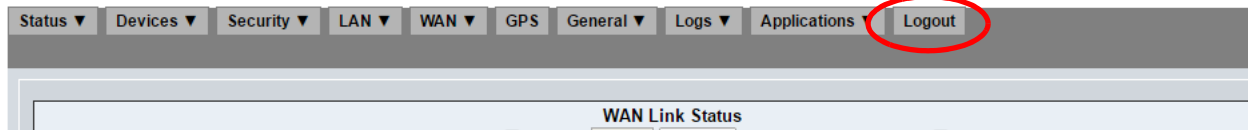


Figure 2-2: Log out of the LCI

2.4 Viewing Only Configuration Settings (Easy Access)

The MG90 includes a read-only Device Easy Access page, which allows users on all devices connected to the unit to view the unit's operational status without logging in to the LCI.

To view the Easy Access page from a device (e.g. laptop) connected to the unit:

1. Launch your browser and enter the router's URL or IP address:
<https://welcome.to.sierrawireless/MG-LCI/easyaccess.html> or <https://172.22.0.1/MG-LCI/easyaccess.html>.
(If the IP address has been changed, replace 172.22.0.1 (the default address) with the updated address.)

Note: The page will appear as unsecured.

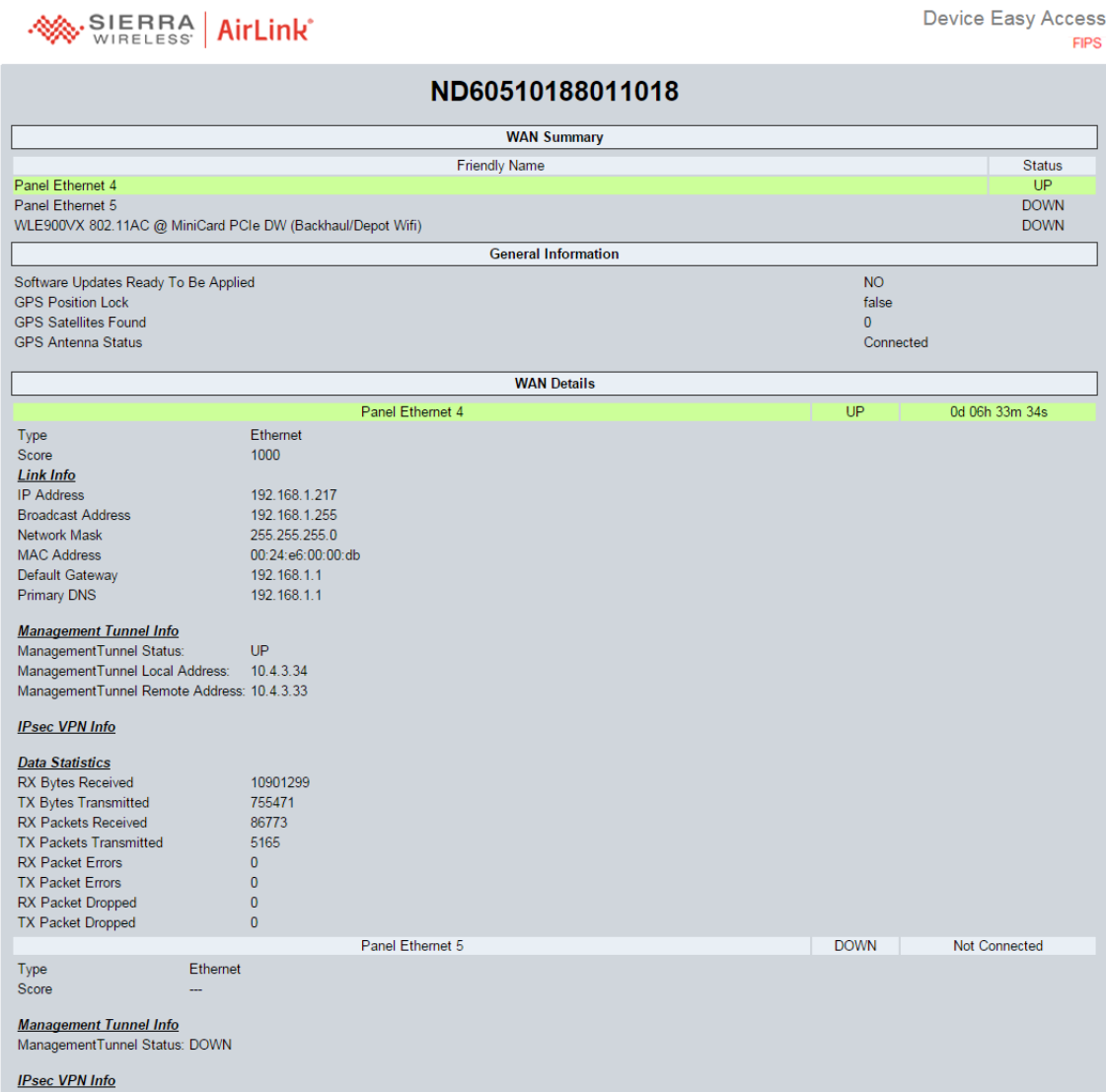


Figure 2-3: Device Easy Access Page

Note: The red 'FIPS' indicator in the top-right portion of the screen appears only if the MG90 uses a FIPS-compliant encryption module.

3: Configuring Startup / Shutdown Behavior

The MG90 startup behavior (automatic or manual) and shutdown behavior (automatic or manual) can be customized options on the LCI's General tab.

3.1 Startup Behavior

The MG90's default configuration is to boot (turn on) automatically (if AutoPower is selected) when ignition is detected. To modify the startup behavior:

1. Go to General > Startup.

The screenshot shows the 'Startup Configuration' window. At the top, there's a navigation bar with tabs: Status, Devices, Security, LAN, WAN, GPS, General (selected), Logs, Applications, and Logout. Below this, there's a sub-navigation bar with tabs: Startup (selected), Shutdown, Services, Tools, Backup/Restore, and Advanced Routing Rules. The main content area is titled 'Startup Configuration'. It contains two settings: 'AutoPower' with a checked checkbox, and 'Delay After Ignition On (secs)' with a text input field containing '5' and a range '(0 secs - 255 secs)'. At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 3-1: Startup Behavior Configuration (LCI: General > Startup)

2. Select / deselect AutoPower as appropriate:
 - Selected — MG90 turns on automatically when ignition is detected.
 - Deselected — MG90 does not turn on automatically. After the vehicle ignition is turned on, the Reset button on the front panel must be pressed to turn the device on.
3. In the Delay After Ignition On field (if AutoPower is selected), enter the delay (in seconds) to wait after turning on the ignition before the MG90 will turn on.
4. Click Save.

For detailed field information, see [General > Startup](#) on page 238.

3.2 Shutdown Behavior

The MG90 automatically shuts down when excessive or insufficient power is detected, or when extreme temperature conditions are encountered (using the unit's built-in temperature sensor).

To modify the shutdown behavior (temperature and voltage thresholds):

1. Go to General > Shutdown.

The screenshot shows the 'Shutdown Configuration' window. At the top, there's a navigation bar with tabs: Status, Devices, Security, LAN, WAN, GPS, General (selected), Logs, Applications, and Logout. Below this, there's a sub-navigation bar with tabs: Startup, Shutdown (selected), Services, Tools, Backup/Restore, and Advanced Routing Rules. The main content area is titled 'Shutdown Configuration'. It contains several settings: 'High Voltage (volts)' (36.0, range 0.0v - 50.0v), 'Low Voltage (volts)' (11.0, range 0.0v - 50.0v), 'Low Voltage Alarm Hysteresis' (0.9, range 0.5v - 1.5v), 'High Temperature (°C)' (85.0), 'Low Temperature (°C)' (-30.0), 'Uptime Extension After Ignition Off (hrs)' (0.25, range 0 - 25.5), and 'Button Reset Time (secs)' (10, range 0 sec - 255 sec). At the bottom, there are 'Save' and 'Cancel' buttons.

Figure 3-2: Shutdown Configuration (LCI: General > Shutdown)

2. Configure the voltage and temperature fields as appropriate.
For example, adjust the Low Voltage value if you want the MG90 to shut down when operating off the vehicle battery and the battery charge is getting too low.
For detailed field information, see [General > Shutdown](#) on page 239.

Note: Voltage readings are subject to cable length and will always be slightly lower than the voltage measured at the source.

3. Click Save.

When the MG90 shuts down due to a high/low voltage or high/low temperature condition, the unit's Power LED turns solid red, and stays red until the condition is resolved. For more information on the MG90's LED patterns, see [LEDs](#) on page 263.

4: Preparing the Network Interfaces

The MG90 is pre-configured with devices that provide LAN and/or WAN connectivity, including LTE or 5G radio modules, Wi-Fi modules, and Ethernet ports.

Before using the MG90, verify the settings for each device to ensure they are properly configured for LAN or WAN data communications. Device types include:

- Cellular devices (e.g. pre-installed MC7354, MC7430/MC7455, EM7511/EM7565, EM9190 radio modules) — See [Configuring Cellular Devices](#) on page 23.
- Ethernet ports (pre-installed ports on rear panel) — See [Configuring Ethernet Ports](#) on page 24.
- Wi-Fi devices (e.g. pre-installed Wi-Fi modules) — See [Configuring Wi-Fi Devices](#) on page 24.
- Serial modem (e.g. Harris Land Mobile Radio) — See [Configuring a Serial Modem Device](#) on page 25.
- Serial port (Device connected to serial port on rear panel) — See [Configuring the Serial Port](#) on page 25.
- Internal Bluetooth device — See [Configuring the Bluetooth Device](#) on page 26.

4.1 Configuring Cellular Devices

To verify and configure cellular device settings:

1. Go to Devices > Cellular:

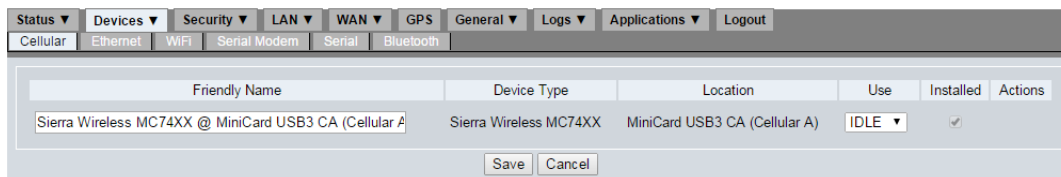


Figure 4-1: LCI: Devices > Cellular

Note: Your MG90 will have 1–2 pre-installed LTE or 5G radio modules (e.g., MC7354, MC7430/MC7455, EM7511/EM7565, EM9190 radio modules).

- a. If desired, enter descriptive names for each device in the Friendly Name fields. (The Friendly Name is used to identify the device in other LCI screens.)
- b. If the Installed field is not marked (checked) for a device that you know is physically installed (has not been temporarily removed), contact Sierra Wireless Technical Support for assistance (see [Contact Information](#) on page 3).
- c. In the Use drop-downs for each device, select the current usage state:
 - WAN — Use the device to connect the MG90 to a mobile network.
 - IDLE — Do not use the device for WAN connections at this time.

Important: *Ensure at least one device is set to WAN so the unit can connect to a network when away from Wi-Fi access points (for example, outside of a depot, away from the depot's access point).*

- d. If you made any changes, click Save.

4.2 Configuring Ethernet Ports

To verify and configure Ethernet port settings:

1. Go to Devices > Ethernet:

Friendly Name	Device Type	Location	Use	Installed	Actions
Panel Ethernet 1	Device Built-in Ethernet Port	Panel Ethernet 1	LAN	☒	
Panel Ethernet 2	Device Built-in Ethernet Port	Panel Ethernet 2	LAN	☒	
Panel Ethernet 3	Device Built-in Ethernet Port	Panel Ethernet 3	LAN	☒	
Panel Ethernet 4	Device Built-in Ethernet Port	Panel Ethernet 4	WAN	☒	
Panel Ethernet 5	Device Built-in Ethernet Port	Panel Ethernet 5	WAN	☒	

Figure 4-2: LCI: Devices > Ethernet

- In the Use drop-downs for each port, select the current usage state:
 - LAN — Use the port to connect a device to the MG90's LAN.
 - WAN — Use the port to connect the MG90 to a WAN.
 - IDLE — Do not use the port to connect devices at this time.
- If the Installed field is not marked (checked) for any of the ports, contact Sierra Wireless Technical Support for assistance (see [Contact Information](#) on page 3).
- If you made any changes, click Save.

4.3 Configuring Wi-Fi Devices

To verify and configure Wi-Fi device settings:

1. Go to Devices > Wi-Fi:

Friendly Name	Device Type	Location	Use	Installed	Actions
WLE900VX 802.11AC @ MiniCard PCIe WiFi A	WLE900VX 802.11AC	MiniCard PCIe WiFi A	WAN	☒	

Figure 4-3: LCI: Devices > Wi-Fi

- In the Use drop-downs for each device, select the current usage state:
 - LAN — Use the Wi-Fi module as an access point ('Vehicle Wi-Fi') for wireless devices to connect to the router. (Wi-Fi B is set to LAN by default.)
 - WAN — Use the Wi-Fi module for 'Depot Wi-Fi', which is used when the MG90 returns to a depot that has a wireless AP available. (Wi-Fi A is set to WAN by default.)
 - IDLE — Do not use the Wi-Fi module at this time.
- If the Installed field is not marked (checked) for a device that you know is physically installed (has not been temporarily removed), contact Sierra Wireless Technical Support for assistance (see [Contact Information](#) on page 3).
- If you made any changes, click Save.

4.4 Configuring a Serial Modem Device

To verify and configure serial modem device settings:

1. If you have a serial modem (Harris Land Mobile Radio) attached to the RS-232 serial port, go to Devices > Serial Modem:

Figure 4-4: LCI: Devices > Serial Port

- a. In the Use drop-down, select one of the following:
 - WAN — Enable the serial modem.
 - IDLE — Do not use the serial modem at this time.
- b. If you made any changes, click Save.

Important: The serial modem can only be used if the serial port 'use' type (in Devices > Serial) is set to 'Application'. See [Configuring the Serial Port](#) on page 25.

4.5 Configuring the Serial Port

To verify and configure the RS-232 DB9 serial port settings:

1. Go to Devices > Serial:

Figure 4-5: LCI: Devices > Serial

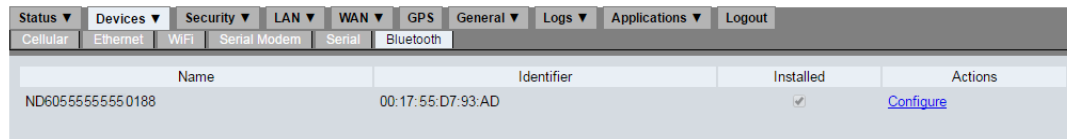
- a. In the Use drop-down, select the port's current usage state:
 - Console — This option should only be selected under the direction of Sierra Wireless Technical Support.
 - Application — Connect the serial port to a device that uses a serial connection (for example, a serial modem (see [Configuring a Serial Modem Device](#) on page 25) or an external GPS device (see [Setting up GPS connectivity](#) on page 94).
 - LAN — Connect the serial port to a Sierra Wireless GNX AirLink Companion device, allowing the device to transfer vehicle telemetry data over the MG90's WAN connection instead of using its own cellular radio module. (See [Configuring the Serial LAN Segment](#) on page 68.)
- b. If you changed the Use value, click Save.

Note: If the Use state is LAN, a "Serial LAN" segment is automatically created in LAN > LAN Segments and associated with the serial port.

4.6 Configuring the Bluetooth Device

To verify and configure the internal Bluetooth device's settings:

1. Go to Devices > Bluetooth:



Status ▾ Devices ▾ Security ▾ LAN ▾ WAN ▾ GPS General ▾ Logs ▾ Applications ▾ Logout			
Cellular Ethernet WiFi Serial Modem Serial Bluetooth			
Name	Identifier	Installed	Actions
ND60555555550188	00:17:55:D7:93:AD	☒	Configure

Figure 4-6: LCI: Devices > Bluetooth

- a. Click Configure in the Actions column.
- b. Configure the fields as appropriate. For detailed field information, see [Bluetooth Adapter Configuration \(Devices > Bluetooth > Configure\)](#) on page 131.
- c. Click Save.

5: Administration

Some typical MG90 administration tasks that you can perform in the LCI include:

- Display MG90 device and WAN status details:
 - See [Displaying General Information](#) on page 27.
 - See [Obtaining WAN Status Details](#) on page 27.
- Configure access to the MG90:
 - See [Configuring User Access](#) on page 30.
 - See [Changing the Root Password](#) on page 32.
- Backup/restore/reset the MG90. See [Backing Up, Restoring, and Factory Resetting the Router](#) on page 33.
- Use advanced tools to manage and troubleshoot the MG90:
 - See [Configuring Services](#) on page 36.
 - See [Using Diagnostic Tools](#) on page 37.
 - See [Running Custom Scripts](#) on page 38.

5.1 Displaying General Information

To display general MG90 details (such as serial number, hardware and software version numbers, voltage, temperature, and basic GPS data):

1. Go to Status > General.

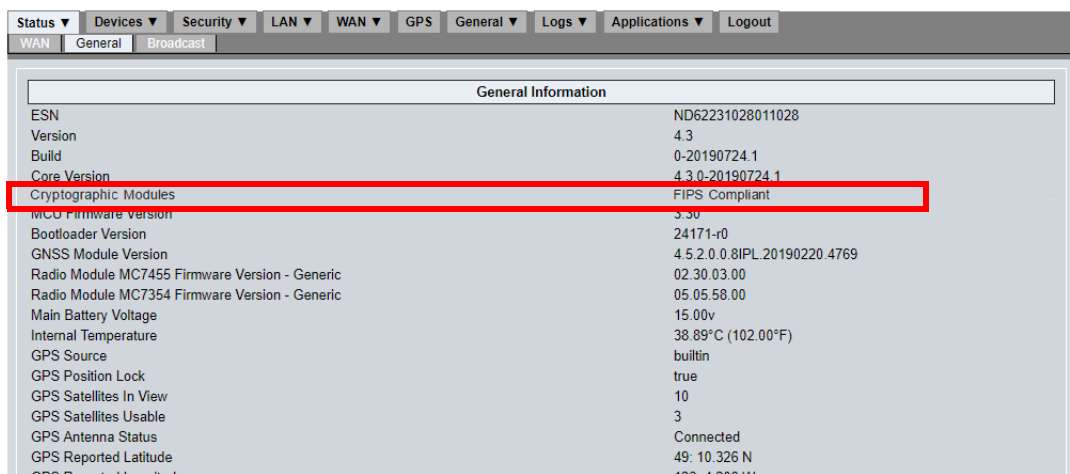


Figure 5-1: LCI: Status > General

Note: The 'Cryptographic modules' entry (shown above) appears only if the MG90 uses a FIPS-compliant encryption module.

For detailed field information, see [General Information](#) on page 120.

5.2 Obtaining WAN Status Details

To display detailed WAN status information, including the MG90's IP address, data transmission statistics, etc.):

1. Go to Status > WAN.

2. Select Show Extended Status.

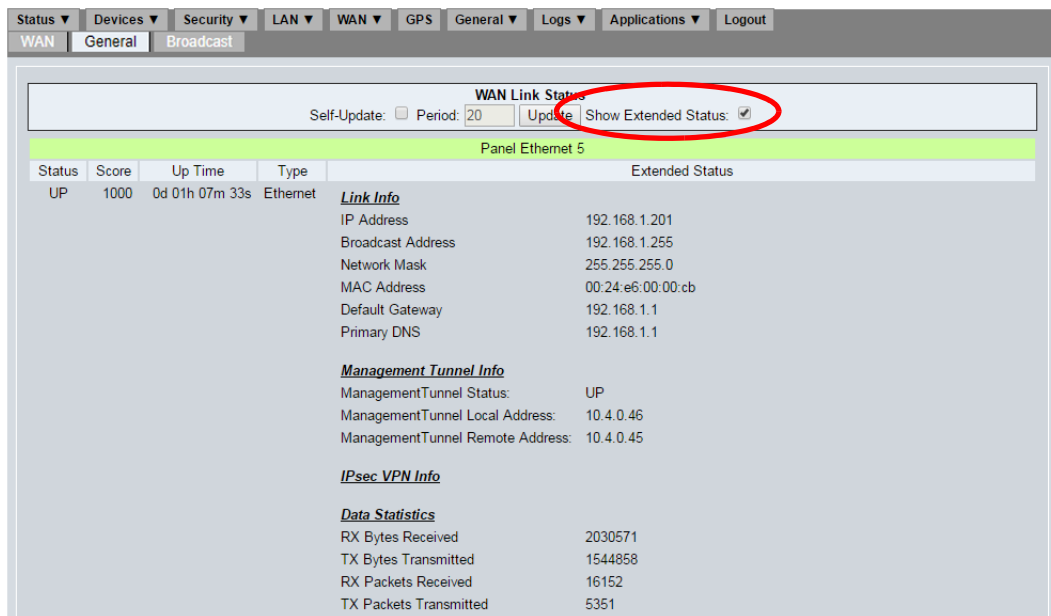


Figure 5-2: LCI: Status > WAN > Extended Status

For detailed field information, see [Extended status screen](#) on page 115.

5.3 Broadcast Router Status

The MG90 can be configured to broadcast device status information (including GPIO, WAN, GNSS, VPN, and general status details) at regular intervals, when GPIO states change, or both. Selected data items are broadcast (in JSON format) on a specific UDP port on one or more LAN segments, and users on those LAN segments can use a network analyzer (e.g. tcpdump) to listen for data packets on the UDP port.

To configure status broadcasting:

1. Go to Status > Broadcast.

Status Broadcast Configuration

Options

Enable ☐

Broadcast Port

LAN Segments ☒ Default LAN 172.22.0.1 ☒ LAN-1 172.22.1.1 ☐ LAN-2 172.22.2.1

Broadcast on Time Interval ☒

Broadcast Interval (ms)

Broadcast on GPIO State Change ☐

GPIO Sampling Interval (ms)

Broadcast on WAN State Change ☐

WAN Sampling Interval (ms)

Broadcast Data

Location ☒

GPIO States ☒

WAN States ☒

WAN Network Type ☒

WAN Signal Strength ☒

Cellular Band Number ☒

Cellular Bandwidth ☒

Cellular RSSI ☒

Cellular RSRP ☒

Cellular RSRQ ☒

Cellular SINR ☒

5G NR Band Number ☒

5G NR Bandwidth ☒

5G NR RSRP ☒

5G NR RSRQ ☒

5G NR SINR ☒

GNSS Status:

GPS Fix ☒

Number of Satellites ☒

GPS Antenna Connected ☒

VPN Status ☒

☒ Combined

☐ Individual

General Status:

Ignition Status ☒

Main Battery Voltage ☒

Figure 5-3: LCI: Status > Broadcast

2. Select Enable to activate the broadcast feature.
3. Set the broadcast scheduling options:
 - a. In the Broadcast Port field, enter the UDP port to use for broadcasting.
 - b. In LAN Segments, select one or more LAN Segments to use for broadcasting.
 - c. To broadcast status details on a regular schedule, select Time Interval Mode and enter the Broadcast Interval (in milliseconds).
 - d. To broadcast status details when the state of any GPIO changes, select Broadcast on GPIO State Change and enter the GPIO Sampling Interval (in milliseconds) at which GPIO states are checked.
 - e. To broadcast status details when the status of any WAN link changes, select Broadcast on WAN State Change and enter the WAN Sampling Interval (in milliseconds) at which WAN link connection states are checked.

Note: At least one of the 'Broadcast options (Broadcast Interval, Broadcast on GPIO State Change, or Broadcast on WAN State Change) must be selected for broadcasting to be enabled. If none are selected, the Enable option is cleared when Submit is clicked.

4. Select the status details to be included in broadcasts:
 - Location (i.e., Latitude and longitude)
 - GPIO States (i.e., GPIO input/output states (all five GPIOs))
 - WAN States (i.e., State of each individual WAN link (includes Friendly Name, Status (0 or 1), Active (true or false), WAN network type and signal strength (in dBm), and Cellular link details (band number, bandwidth, RSSI (in dBm), RSRP (in dBm), RSRQ (in dB), SINR (in dB)))
 - GPS Fix (i.e., Fix available (true or false))
 - Number of Satellites (i.e., Number of usable satellites)
 - GPS Antenna Connected (i.e., True or false)
 - VPN Status (i.e., Combined (General VPN status indicating 0 (none active) or 1 (at least 1 VPN is up)), or Individual (each VPN's Friendly Name and status (0 — Down or 1 — Up)))
 - Ignition Status (i.e., True or false)
 - Main Battery Voltage (i.e., Voltage, in volts)
 - Internal Temperature (i.e., Temperature, in °C)
5. Click Submit. The selected Broadcast Data details are compiled into a JSON-formatted file and broadcast over UDP based on the selected Options. (For the JSON schema and an example, see [JSON Data](#) on page 265.)

For detailed field information, see [Status Broadcast](#) on page 123.

5.4 Configuring User Access

By default, the LCI includes one Administrator-type user account ('admin'). Additional accounts (user names) can be created with the following user types:

- Administrator — Administrator users can access and update all screens in the LCI.
- User — Regular Users can view the basic status information (WAN > Status), but not make any changes in the LCI.

Note: User names are case-sensitive.

Important: *Sierra Wireless recommends that you create strong, unique passwords for each Administrator-type account on each MG90 to prevent unauthorized access to the device. Make sure the username and password are different, otherwise a warning dialog to remind you will appear at each login until the password is changed.*

Usage note for AMM — The password and login name requirements described below also apply when setting up users via AMM. However AMM does not enforce these requirements. It is important to follow these requirements so newly-added users will be able to access the LCI.

Adding Users

To add a new user account:

1. Go to Security > Users.

User Name	Role	Action
admin	Administrator	Edit Delete
user	User	Edit Delete

Figure 5-4: LCI: Security > Users

2. Enter the Login Name (username) that will be used to log in to the LCI.
Requirements: Length = 2–28 characters; Allowed characters: 'A'–'Z', 'a'–'z', '0'–'9', period ('.'), underscore ('_') and hyphen ('-')
3. Enter a Password for the account.
Password requirements: minimum length = 8; must contain at least one uppercase ('A'–'Z'), one lowercase ('a'–'z') and one numeric ('0'–'9')
4. In Confirm Password, re-enter the password for the account.
5. In the Role drop-down, select the account type:
 - Administrator — Select if the user needs full access to the LCI.
 - User — Select if the user needs only to view MG90 status details.
6. Click Add User.

Important: Make sure there is always at least one user with the 'Administrator' role before logging out or disconnecting. If there are no administrators remaining, the LCI will not be accessible and the MG90 will require a factory reset to regain access.

Updating Users

To modify an existing user account's password:

1. Go to Security > Users.
2. Click Edit in the Action column for the account to modify.
3. Modify the Password field and Confirm Password fields.
4. Click Edit User.

Deleting Users

To delete a user account:

1. Go to Security > Users.
2. Click Delete in the Action column for the account.
3. Click OK when prompted to confirm the deletion.

For detailed field information, see [Security > Users](#) on page 133.

Important: Make sure there is always at least one user with the 'Administrator' role before logging out or disconnecting. If there are no administrators remaining, the LCI will not be accessible and the MG90 will require a factory reset to regain access.

5.5 Changing the Root Password

The MG90 can be remotely accessed for advanced diagnostics by your IT department or Sierra Wireless Technical Support by using a root password.

Important: Sierra Wireless recommends that you create strong, unique root passwords for each MG90 to prevent unauthorized users from changing router settings. You will need to provide the password to authorized users who need to access the MG90.

Important: If you forget the root password, it cannot be recovered. You must perform a factory reset to restore it to the default value. See [Factory resetting the configuration](#) on page 35 for details. If you do not know the default root password, contact Sierra Wireless Technical Support for assistance (see [Contact Information](#) on page 3).

To change the root password:

1. Go to Security > Change Root Password.

Figure 5-5: LCI: Security > Change Root Password

2. Enter the Old root password.
3. Enter the New root password.
Password requirements: minimum length = 8; must contain at least one uppercase ('A'–'Z'), one lowercase ('a'–'z') and one numeric ('0'–'9')
4. Re-enter the new password to confirm.
5. Click Change.

For detailed field information, see [Security > Change Root Password](#) on page 134.

5.6 Configuring Supported LCI Access Protocols

By default, the LCI is accessed from a browser using HTTPS only.

If unsecured access is required, the URI scheme can be modified to also allow HTTP access.

To change the supported LCI access protocols:

1. Go to Security > Settings.

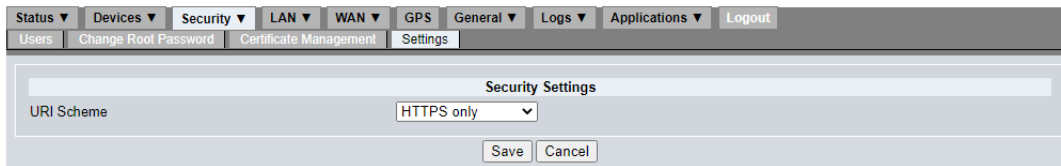


Figure 5-6: LCI: Security > Settings

2. From the URI Scheme dropdown, select:
 - HTTPS only— LCI must be accessed using HTTPS.
 - HTTP and HTTPS— Either protocol can be used to access the LCI. Different LAN segments can use either method.
3. Click Save.
4. If the URI scheme was changed from "HTTPS only" to "HTTP and HTTPS", clear the browser cache before attempting to log in using HTTP.

For detailed field information, see [Security > Settings](#) on page 140.

5.7 Backing Up, Restoring, and Factory Resetting the Router

MGOS provides the ability to manually save, restore, and reset configuration settings if required:

- Save (back up) the router's current configuration (multiple backups can be saved)
- Restore the router to a previously saved configuration
- Factory reset— Reset the configuration to factory default settings (optionally keeping selected 'core' settings unchanged)

Important: If you have an AMM (AirLink Mobility Manager) account through Sierra Wireless (or operate your own AMM server), the current configuration is saved automatically each time the MG90 connects to the AMM account (and a history of configuration changes is saved). This copy of the configuration file can be restored to the router if needed.

AMM can also be used to build and deploy configuration updates to multiple routers. However, it should not be used to deploy the configuration file from one MG90 to other devices due to different potential impacts on various application and hardware-specific settings. Refer to your AMM documentation for instructions.

Important: When a saved configuration is used to restore a router (the same router, or a replacement device):

- Configuration backups do not save certificates, CSRs, or legacy certificate private keys.
- Users are responsible for keeping their own backups of legacy certificates and private keys.
- If restoring a router after a full factory reset, or loading configuration to a new router, new CSRs must be generated to obtain new certificates. For legacy certificates, the user is responsible for reloading the certificates and keys from their own backups.

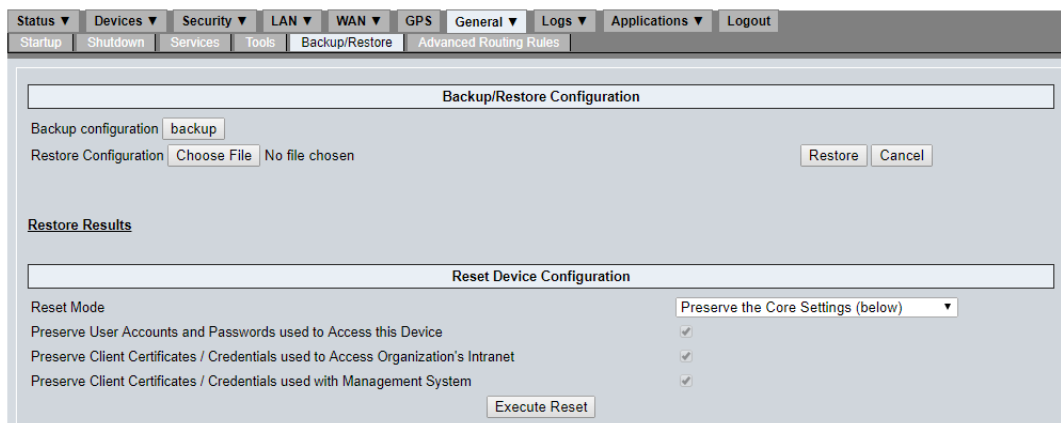


Figure 5-7: LCI: General > Backup/Restore

For detailed field information, see [General > Backup/Restore](#) on page 244.

5.7.1 Backing up the current configuration

To back up the MG90's configuration:

1. Go to General > Backup/Restore.
2. Click backup. The configuration file saves automatically to your default downloads folder.
3. In Windows Explorer, move the configuration file from the downloads folder to a folder where you want to save your backup files.

Tip: Sierra Wireless recommends renaming the saved backup file to include the MGOS version number, so the correct version can easily be found and restored if necessary (see [Restoring an earlier configuration](#), below). See [Displaying General Information](#) on page 27 to view an MG90's version information.

5.7.2 Restoring an earlier configuration

Important: Before you restore a configuration to the MG90, ensure the MGOS software version currently running matches the version that was running when the original configuration file was created—if they don't match, the MG90 may not function properly. See [Displaying General Information](#) on page 27 to view an MG90's version information.

To restore a configuration from a previous backup:

1. Go to General > Backup/Restore.
2. Click Choose File / Browse. (The button label depends on the browser being used. Typically, the label is Choose File or Browse.)
3. Navigate to the folder containing your backup files.

4. Select the appropriate backup file and click OK.
The fully qualified filename appears in the Restore Configuration field.

Note: If you decide not to restore the selected backup file, click Cancel.

5. Click Restore. When the restoration is complete, comprehensive details appear in the Restore Results section.

5.7.3 Factory resetting the configuration

The router's configuration can be fully reset to factory default values, or some core settings can be retained if needed. Core settings include user accounts and passwords, and client certificates / credentials for certificate authentication.

There are two methods for initiating a factory reset:

- Software reset — Use the Reset Device Configuration fields as described below.
- Hardware reset — Refer to [1] AirLink MG90 Hardware User Guide for details.

Warning: *The hardware reset is a full reset, equivalent to a software reset with Reset All to Factory Defaults selected.*

To reset the configuration (software reset):

1. Go to General > Backup/Restore.
2. From the Reset Mode dropdown list, select:
 - Preserve the Core Settings (below) — Select this option to save all core settings. All other configurations will reset to factory defaults.
 - Preserve Selected Core Settings (below) — Select this option to be able to choose which of the core settings should be saved. All other configurations will reset to factory defaults.
 - Reset All to Factory Defaults — Select this option to reset all configurations to factory defaults. None of the core settings will be saved.
3. If the Reset Mode is set to Preserve Selected Core Settings, select any / all of the core setting types to save:
 - Preserve User Accounts and Password used to Access this Device — Note that if these are not preserved, only the Admin account will be available after the reset.
 - Preserve Client Certificates / Credentials used to Access Organization's Intranet — These are the certificates that have previously been loaded into the device either manually or by being pushed from AMM. If not preserved, new certificates must be loaded to access VPNs or Wi-Fi networks that use certificate authentication.
 - Preserve Client Certificates / Credentials used with Management System — Reserved for future use with AMM. This field is not currently accessible.
4. Click Execute Reset.
5. When prompted to confirm the reset, click OK.
The router will reboot with factory settings restored (except for any core settings that were selected to preserve).

5.7.4 AMM-Initiated Multiple Unit Reboot

(Applies to MG90 routers running MGOS 4.4.1 or later)

MG90 routers support the AMM multiple unit reboot feature, which allows AMM to initiate an unscheduled mass reboot for MG90 routers. Note that the multiple unit reboot feature is available on AMM 2.17.2 and newer.

The router will automatically reboot when it receives the request from AMM. (This reboot cannot be cancelled.)

5.8 Configuring Services

The Device Service Configuration screen (General > Services) is used to configure event reporting, the Wi-Fi country code broadcast by Wi-Fi, and network NTP.



Figure 5-8: LCI: General > Services—Sample screen

For detailed field information, see [General > Services](#) on page 240.

5.8.1 Configuring Event Reporting

Events generated on the MG90 are reported to AMM. By default, AMM's address is provided to the MG90 by DNS servers managed by Sierra Wireless.

Recommendation: These settings should only be modified as directed by Sierra Wireless.

To view and configure event reporting settings:

1. Go to General > Services.
2. If necessary, modify appropriate settings.
3. Click Save.

5.8.2 Enabling the Legacy Beacon Service

The beacon service can be enabled to send a signal to the LAN to indicate the current WAN status (up or down).

Recommendation: Use the Status Broadcast feature (Status > Broadcast) instead of this legacy feature, since the broadcast feature provides more complete status information. See [Broadcast Router Status](#) on page 28 for details.

To enable/disable the legacy beacon service:

1. Go to General > Services.
2. Select Enable Beacon Service (or deselect to disable).
3. Click Save.

5.8.3 Configuring Wi-Fi Country Code

The Wi-Fi country code must be set to the country in which the router is currently being operated. This is required to ensure the router's Wi-Fi radio settings conform to relevant national regulations.

Recommendation: *This setting should only be changed if the router is to be used in a different country.*

To change the Wi-Fi country code:

1. Go to General > Services.
2. Select the new country from the WiFi Country Code dropdown.
3. Click Save.

5.8.4 Configuring NTP Servers

By default, Network NTP is enabled, which ensures devices on the network are properly synchronized via network NTP servers.

Default NTP servers can be used, or alternate servers (typically managed by the organization) can be specified.

Note: When upgrading from MGOS 4.2.x or earlier to MGOS 4.3 or later, any existing NTP server configuration that was manually stored in `ntp.conf:template` will be converted and stored in the Alternate Network NTP Servers list.

To configure the router's NTP server details:

1. Go to General > Services.
2. If NTP synchronization is to be used, select Enable Network NTP.
3. Choose which NTP servers to use:
 - To use the default NTP servers, select Use Network NTP Default Servers.

Note: Default servers are:

- `0.north-america.pool.ntp.org`
 - `1.north-america.pool.ntp.org`
 - `2.north-america.pool.ntp.org`
-

- To use your organization's NTP servers, deselect Use Network NTP Default Servers and then enter the server names in the Alternate Network NTP Servers frame.

4. Click Save.

5.9 Using Diagnostic Tools

The MG90 includes several command line diagnostic tools to help with upgrading, provisioning, and troubleshooting.

To use a diagnostic tool:

1. Go to General > Tools.
2. Select the tool to use in the Command drop-down. For descriptions of available tools, see [General > Tools](#) on page 242.

3. Enter any command line arguments to use with the tool in the Arguments field (see [Figure 5-9](#) for a 'ping' example).
4. Click Execute. If the tool produces an output it appears under Results.

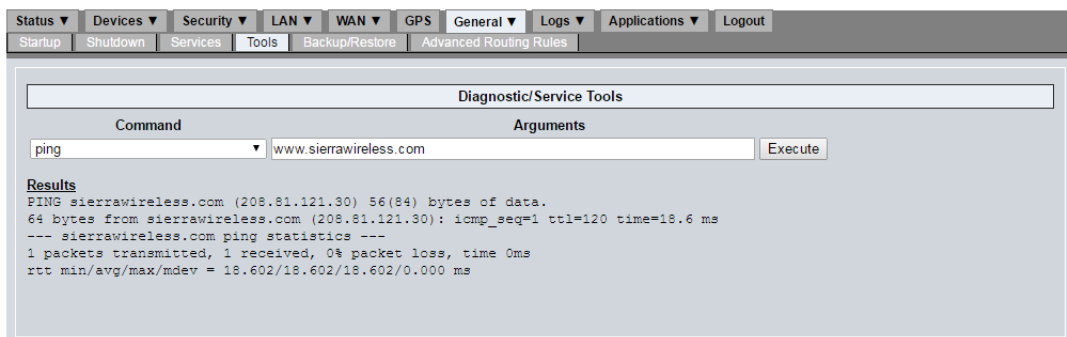


Figure 5-9: Tool example—ping

5.10 Running Custom Scripts

Administrators (e.g. your IT department or Sierra Wireless Technical Support) can run custom scripts on the MG90 to perform advanced functionality and device customization. These scripts are run from the General > Advanced Routing Rules tab.

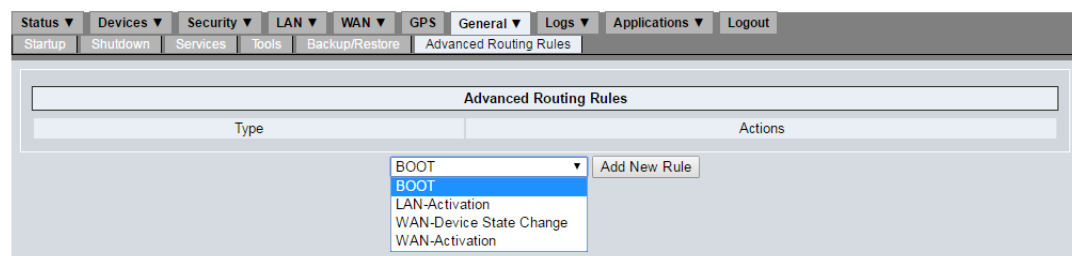


Figure 5-10: Advanced Routing Rules Screen

This should only be attempted by individuals who are proficient with Linux shell scripting and when a result cannot be achieved using the standard configuration measures available from the LCI.

Important: Since incorrect use of this feature may disable the unit, Sierra Wireless recommends that such configuration be done in consultation with Sierra Wireless Technical Support.

For detailed option information, see [General > Advanced Routing Rules](#) on page 245.

6: Setting Up The WAN

The MG90 can connect to the WAN using three device types:

- Cellular—Typically used when the vehicle is traveling outside the area around its depot.
- Wi-Fi—Typically used when the vehicle returns to a depot that has an AP available for the MG90 to connect to as a client.
- Ethernet—By default, Port 5 is configured for WAN access, and Ports 1–4 are configured for LAN access.

Multiple devices can be active (configured for WAN) at the same time to provide redundant WAN access should one or more connections go down.

Note: The MG90 does not support USB-to-Ethernet adapters for WAN operation.

6.1 Basic WAN Link Configuration

Each device that is currently configured for WAN connectivity is listed as a WAN link on the WAN > Links tab. (See [Preparing the Network Interfaces](#) on page 23 to configure devices for WAN use.)

Note: If a device (such as a cellular radio) was removed from the MG90 while it was configured for WAN usage, it appears in this list with the 'Enabled' flag not selected and will have a Delete option in the Actions column.

To configure the settings for a WAN link:

1. Go to WAN > Links.

Friendly Name	Device Type	Enabled	Actions
My Harris Land Mobile Radio	TTY Serial Port	☒	Configure Policies Networking Rules
Panel Ethernet 1	Device Built-in Ethernet Port	☒	Configure Policies Networking Rules
Panel Ethernet 5	Device Built-in Ethernet Port	☒	Configure Policies Networking Rules
Sierra Wireless MC74XX @ MiniCard USB3 CA (Cellular A)	Sierra Wireless MC74XX	☒	Configure Policies Networking Rules
WLE900VX 802.11AC @ MiniCard PCIe WiFi A	WLE900VX 802.11AC	☒	Configure Policies Networking Rules
WLE900VX 802.11AC @ MiniCard PCIe WiFi B	WLE900VX 802.11AC	☐	Delete Configure Policies Networking Rules

Figure 6-1: WAN > Links Tab

2. Click Configure in the Actions column for the link.
3. Configure the link using the appropriate procedure:
 - Cellular link—See [Cellular WAN Link Configuration](#) on page 40.
 - Wi-Fi link—See [Wi-Fi WAN Link Configuration](#) on page 43.
 - Ethernet link—See [Ethernet WAN Link Configuration](#) on page 43.
 - Serial link—See [Serial WAN Link Configuration](#) on page 45.

6.1.1 Cellular WAN Link Configuration

Cellular WAN links provide connectivity wherever cellular reception is available. The Cellular WAN Link Configuration screen allows you to view and modify connection settings for an installed cellular radio module with an activated SIM installed.

In the Cellular WAN Link Configuration screen (see [Figure 6-3](#) below):

1. Configure the fields for the selected cellular device. For detailed field information, see [Cellular WAN Link Configuration](#) on page 176.

Warning: In the VPN field, if a VPN profile is selected that is configured as a full tunnel (subnet 0.0.0.0/0), **do not** select any other profiles. If the full tunnel profile **and** another profile are selected, none of the changes made to the screen will be saved when Save is clicked.

Tip: If the WAN link is a private network that requires a user name and password for access, enter the following command in the Advanced Modem Initialization String field:

`AT$QCPDPP=1\,1\,<password>\,<username>`

For example:

`AT$QCPDPP=1\,1\,3AD29482\,6045551234@static.carrier.ca`

2. Click Save.

For information on specific settings for your card, contact your carrier or visit <http://source.sierrawireless.com>.

Note: The fields displayed vary depending on cellular radio module type and LCI settings.

Status ▾ Devices ▾ Security ▾ LAN ▾ **WAN ▾** GPS ▾ General ▾ Logs ▾ Applications ▾ Logout
 Links Monitors VPNs WiFi Networks Networking Rules Recovery SIM Configuration

Cellular WAN Link Configuration

(Sierra Wireless MC74XX @ MiniCard USB3 CA (Cellular A))

High Cost Link	☐
MTU Size	☒ Automatic ☐ Manual
Enable TCP MSS Clamping	☒
Masquerade	☒
Masquerade Port Range	☐ Automatic ☒ Manual Minimum Port Number 49152 Maximum Port Number 65535
Automatic DNS	☒
Primary DNS	
Secondary DNS Servers	comma-separated IP addresses
Enable Private Zone	☐
Number of Private Zone:	1 ▾
APN	sp.telus.com
Allow Blank APN	☐
Signal Strength Filter Length	10
Signal Strength Change Threshold (dBm)	5
Setting for Band	All Bands ▾
Custom Band Setting Mode	Exclude Bands ▾ 4 comma-separated bands
Use Management Tunnel	☒
Pilot Ping	☐
Monitors	☒ DefaultMonitor
Monitor Mode	Success in one monitor keeps the link up ▾
VPN	☐ VPN Configuration ☐ VPN Configuration_1 ☐ VPN Configuration_2 Connection Method ☐ Connect One ☐ Random ☐ Round Robin - Alphanumeric Order ☒ Connect All
Load Balanced	☐
Weight (1-256)	1
Split Access	☐
Enable Advanced Module Recovery	☒
Recovery Interval (minutes)	10
Advanced Modem Initialization	~ Comma separated
Preferred Mode	☒ Automatic ☐ LTE Disabled
Enable IPV6	☐

Figure 6-2: Cellular WAN Link Configuration (LCI: WAN > Links > Configure)—4G Cellular

Cellular WAN Link Configuration
(Sierra Wireless EM919X @ MiniCard USB3 CA (Cellular A))

High Cost Link ☐

MTU Size ☒ Automatic
☐ Manual

Enable TCP MSS Clamping ☒

Masquerade ☒

Masquerade Port Range ☐ Automatic
☒ Manual
Minimum Port Number 49152
Maximum Port Number 65535

Automatic DNS ☒

Primary DNS

Secondary DNS Servers comma-separated IP addresses

Enable Private Zone ☐

Number of Private Zone: 1

APN m2minternet.apn

Allow Blank APN ☐

Signal Strength Filter Length 10

Signal Strength Change Threshold (dBm) 5

Setting for Band All Bands

Custom Band Setting Mode Exclude Bands
4,12 comma-separated bands

Use Management Tunnel ☒

Pilot Ping ☐

Monitors ☒ DefaultMonitor

Monitor Mode Success in one monitor keeps the link up

VPN

Connection Method ☐ Connect One
☐ Random
☐ Round Robin - Alphanumeric Order
☐ Connect All

Load Balanced ☐

Weight (1-256) 1

Split Access ☐

Enable Advanced Module Recovery ☒

Recovery Interval (minutes) 10

Advanced Modem Initialization ~ Comma separated

Enable IPV6 ☐

Network Type Auto

MIMO Configuration 2x2

Figure 6-3: Cellular WAN Link Configuration (LCI: WAN > Links > Configure) — 5G Cellular

6.1.1.1 Private Network Configuration

The MG90 provides configuration options to support the use of private networks.

A router that is configured to use a private network will use it when in the private networks' coverage area. If the router leaves the coverage area, the link will not fall back to a public network. Rather, an alternate WAN link (e.g. another cellular connection, Wi-Fi connection, etc.) with the next highest priority will be selected (i.e. existing WAN link behavior is followed).

To configure an MG90 to use a private network, go to the Cellular WAN Link Configuration screen (see [Figure 6-3](#) above) for the appropriate link such as an EM7511/EM7565 link or EM9190 link:

1. If the network requires a blank APN to be used:
 - a. Clear the APN field.

- b. Select Allow Blank APN. When these options are saved, the APN will be cleared on the radio module.
2. From the Setting for Band dropdown, select All Bands, LTE ALL. or 5G NR ALL. Note that 5G NR ALL is available only with MG90 5G routers.
3. From the Custom Band Setting Mode, select Restrict to Bands.
4. In the next field (for comma separated bands), enter the network's supported bands.
5. Click Save.

6.1.2 Wi-Fi WAN Link Configuration

Wi-Fi WAN links provide WAN access via Wi-Fi access points (AP), which are often available in locations such as vehicle depots. These links are usually configured as the primary WAN access method, since it is usually preferable to utilize an AP when available. The Wi-Fi WAN Link Configuration screen allows you to view and modify connection settings for the MG90's Wi-Fi modules.

In the Wi-Fi WAN Link Configuration screen (see [Figure 6-4](#) below):

1. Configure the fields for the selected Wi-Fi device. For detailed field information, see [Wi-Fi WAN Link Configuration](#) on page 184.
2. After configuring a Wi-Fi WAN link, select the AP profile(s) that this Wi-Fi WAN link will connect to. (The AP profiles store credentials and other information required to communicate with an AP. See [Defining an Access Point Profile for Wi-Fi Links](#) on page 46 for details.)
3. Click Save.

The screenshot displays the 'WiFi WAN Link Configuration' window. At the top, there's a title bar with tabs: Status, Devices, Security, LAN, WAN (selected), GPS, General, Logs, Applications, and Logout. Below this is a sub-menu bar with: Links, Monitors, VPNs, WiFi Networks, Networking Rules, Recovery, and SIM Configuration. The main content area is titled 'WiFi WAN Link Configuration (WLE900VX 802.11AC @ MiniCard PCIe WiFi A)'. It contains several settings: 'Enable Broadcast Probe' (checked), 'Association Settling Period (s)' (15), 'Disassociation Settling Period (s)' (15), 'Background Scanning Interval (s)' (300), 'Signal Strength Average Length' (10), 'Roaming Squelch' (checked), 'Minimum Quality of Signal (dB)' (8), 'Satisfactory Quality of Signal (dB)' (25), 'Minimum Quality of Signal Differential (dB)' (3), and 'Permanent Blacklist' (empty text field). At the bottom, there's a 'WiFi Networks' section with a checked 'Depot AP' checkbox and an unchecked 'WiFi network 1' checkbox. 'Save' and 'Cancel' buttons are at the bottom right.

Figure 6-4: Wi-Fi WAN Link Configuration (LCI: WAN > Links > Configure)

6.1.3 Ethernet WAN Link Configuration

An Ethernet (wired) connection can also be used to provide WAN access to the MG90, though this is less common since the main purpose of the MG90 is to provide mobile WAN access using wireless methods.

In the Ethernet WAN Link Configuration screen (see [Figure 6-5](#) below):

1. Configure the fields for the selected Ethernet device. For detailed field information, see [Ethernet WAN Link Configuration](#) on page 171.

Warning: In the VPN field, if a VPN profile is selected that is configured as a full tunnel (subnet 0.0.0.0/0), **do not** select any other profiles. If the full tunnel profile **and** another profile are selected, none of the changes made to the screen will be saved when Save is clicked.

2. Click Save.

The screenshot displays the 'Ethernet WAN Link Configuration' window for 'Panel Ethernet 5'. The interface includes a top navigation bar with tabs for Status, Devices, Security, LAN, WAN (selected), GPS, General, Logs, Applications, and Logout. Below this is a sub-navigation bar with links for Links, Monitors, VPNs, WiFi Networks, Networking Rules, Recovery, and SIM Configuration. The main configuration area contains the following settings:

- High Cost Link: ☐
- Change Default MTU Size: ☐
MTU Size: 1500
- Auto Local IP: ☒
- DHCP Assumes Same Network: ☐
- Send Hostname with DHCP: ☒ Disabled, ☐ Send ESN, ☐ Custom
- Local IP Address: [text field]
- Network Mask: [text field]
- Gateway: [text field]
- Masquerade: ☒
- Masquerade Port Range: ☐ Automatic, ☒ Manual
Minimum Port Number: 49152, Maximum Port Number: 65535
- Automatic DNS: ☒
- Primary DNS: [text field]
- Secondary DNS Servers: [text field] (comma-separated IP addresses)
- Enable Private Zone: ☐
- Number of Private Zone: 1
- Use Management Tunnel: ☒
- Pilot Ping: ☐
- Monitors: ☒ DefaultMonitor
- Monitor Mode: Success in one monitor keeps the link up
- VPN: ☒ VPN Configuration, ☒ VPN Configuration_1, ☐ VPN Configuration_2
Connection Method: ☒ Connect One (Random, Round Robin - Alphanumeric Order), ☐ Connect All
- Load Balanced: ☐
Weight (1-256): 1
- Split Access: ☐

At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure 6-5: Ethernet WAN Link Configuration (LCI: WAN > Links > Configure)

6.1.3.1 Setting up PPPoE WAN

A StarTech USB2100 USB-Ethernet adapter can be connected to an available USB slot on the back panel of the MG90 to support a PPPoE WAN link to a connected LMR (Land Mobile Radio) such as a Motorola HPD radio.

Note: Only one adapter can be used.

To set up the MG90:

1. Power off the MG90.

2. Attach the StarTech USB2100 USB-Ethernet adapter to an available USB slot on the back panel.
3. Connect the Ethernet end of the adapter to the PPPoE server device (e.g. the Motorola HPD radio).
4. Power on the MG90.

The connected device will appear on the WAN Link Status screen (Status > WAN) with Status=UP and Type=Ethernet.

6.1.4 Serial WAN Link Configuration

The MG90's serial port can be used to connect a serial modem (Harris Land Mobile Radio) WAN device that has been set up as described in [Configuring the Serial Port](#) on page 25 and [Configuring a Serial Modem Device](#) on page 25.

The Serial WAN Link Configuration screen allows you to view and modify connection settings for the serial modem.

In the Serial WAN Link Configuration screen (see [Figure 6-6](#) on page 46):

1. Configure the fields for the serial modem. See [Serial \(Modem\) WAN Link Configuration](#) on page 185 for details.

Warning: *In the VPN field, if a VPN profile is selected that is configured as a full tunnel (subnet 0.0.0.0/0), **do not** select any other profiles. If the full tunnel profile **and** another profile are selected, none of the changes made to the screen will be saved when Save is clicked.*

2. Click Save.

Serial WAN Link Configuration
(Harris Land Mobile Radio)

High Cost Link ☐

Change Default MTU Size ☐

MTU Size

Auto Local IP ☒

Local IP Address

Masquerade ☒

Masquerade Port Range ☐ Automatic ☒ Manual

Minimum Port Number

Maximum Port Number

Automatic DNS ☒

Primary DNS

Secondary DNS Servers comma-separated IP addresses

Auto Remote IP ☒

Remote IP Address

Serial Modem Speed (bauds)

Modem Initialization

Dial String

Use Management Tunnel ☒

Pilot Ping ☐

Monitors ☒ DefaultMonitor

Monitor Mode

Call Down Recovery ☐

Recovery Time (seconds)

VPN ☒ VPN Configuration ☒ VPN Configuration_1 ☐ VPN Configuration_2

Connection Method ☒ Connect One ☐ Random ☐ Round Robin - Alphanumeric Order ☐ Connect All

Enable Custom txqueuelen ☐

txqueuelen value

Save Cancel

Figure 6-6: Serial WAN Link Configuration (LCI: WAN > Links > Configure)

6.2 Defining an Access Point Profile for Wi-Fi Links

Access Point (AP) profiles must be created for each Wi-Fi AP that the MG90 will use to access the WAN (for example, an AP at a depot). An AP profile contains the settings and credentials required for the MG90 to connect to the AP (for example, access, security, network settings, etc.). These settings must match the settings defined at the actual Wi-Fi AP.

To define and use an AP profile:

1. Define the AP profile:
 - a. Go to WAN > WiFi Networks.

Warning: In the VPN field, if a VPN profile is selected that is configured as a full tunnel (subnet 0.0.0.0/0), **do not** select any other profiles. If the full tunnel profile **and** another profile are selected, none of the changes made to the screen will be saved when Save is clicked.

- b. Click Add New WiFi Network. The WiFi Network Configuration screen appears.

Status ▾ Devices ▾ Security ▾ LAN ▾ WAN ▾ GPS ▾ General ▾ Logs ▾ Applications ▾ Logout

Links Monitors VPNs WiFi Networks Networking Rules Recovery SIM Configuration

WiFi Network Configuration

General Settings:

Friendly Name: WiFi network #1
 SSID: MyWiFi9823
 Probe Hidden SSID: ☒
 Any BSSID: ☒
 BSSID:
 Default Network Priority: ☒
 Priority: 0

Security Settings:

Protected Management Frames: Disabled ▾
 Encryption: WPA-AES/CCMP ▾
 Authentication: WPA-PSK ▾
 PEAP Version: Version 0 ▾
 PEAP Label: Client EAP Encryption (old) ▾
 PEAP Inner Authentication: MSCHAPv2 ▾
 WEP Key Size: 40 bits ▾
 WEP Key:
 Retype WEP Key:
 WPA Pre-Shared Key: ⓘ
 Retype WPA Pre-Shared Key: ⓘ
 Identity: abcdef
 Password:
 Retype Password:
 CA Certificate: Choose File No file chosen (installed)
 Uninstall CA Certificate: ☐
 Certificate Profile: ☒ J-Cert ☐ W-Cert ☐ default-Cert

Network Settings:

High Cost Link: ☐
 Change Default MTU Size: ☐
 MTU Size: 1500
 Auto Local IP: ☒
 DHCP Assumes Same Network: ☐
 Send hostname with DHCP: ☒ Disabled ☐ Send ESN ☐ Custom
 Local IP Address:
 Network Mask:
 Gateway:
 Masquerade: ☒
 Masquerade Port Range:
☒ Automatic ☒ Manual
 Minimum Port Number: 49152
 Maximum Port Number: 65535
 Automatic DNS: ☒
 Primary DNS:
 Secondary DNS:
 Use Management Tunnel: ☒
 Pilot Ping: ☐
 Monitors: ☒ DefaultMonitor
 Monitor Mode: Success in one monitor keeps the link up ▾
 VPN: ☒ VPN Configuration ☒ VPN Configuration_1 ☐ VPN Configuration_2
 Connection Method: ☐ Connect One ☐ Random ☐ Round Robin - Alphanumeric Order ☒ Connect All
 Split Access: ☐

Private Zone:

Enable Private Zone: ☒
 Number of Private Zone: 2 ▾

Private Zone	Private Zone IP	Private Zone IP	
Private Zone 1	testzone1.com	11.11.11.11	Delete
Private Zone 2	testzone2.com	22.22.22.22	Delete

Radio Frequency:

Band	Channels
☒ All	All
☐ 802.11a/n/ac	☐ All ☐ 36 : 5.18 GHz ☐ 40 : 5.2 GHz ☐ 44 : 5.22 GHz ☐ 48 : 5.24 GHz ☐ 149 : 5.745 GHz ☐ 153 : 5.765 GHz ☐ 157 : 5.785 GHz ☐ 161 : 5.805 GHz ☐ 165 : 5.825 GHz
☐ 802.11b/g/n	☐ All ☐ 1 : 2.412 GHz ☐ 2 : 2.417 GHz ☐ 3 : 2.422 GHz ☐ 4 : 2.427 GHz ☐ 5 : 2.432 GHz ☐ 6 : 2.437 GHz ☐ 7 : 2.442 GHz ☐ 8 : 2.447 GHz ☐ 9 : 2.452 GHz ☐ 10 : 2.457 GHz ☐ 11 : 2.462 GHz ☐ 12 : 2.467 GHz ☐ 13 : 2.472 GHz ☐ 14 : 2.484 GHz
☐ Public Safety	5MHz Only ☐ All ☐ 35 : 4.957 GHz ☐ 70 : 4.975 GHz ☐ 65 : 4.972 GHz ☐ 5 : 4.942 GHz ☐ 10 : 4.945 GHz ☐ 40 : 4.96 GHz ☐ 75 : 4.977 GHz ☐ 15 : 4.947 GHz ☐ 45 : 4.962 GHz ☐ 85 : 4.982 GHz ☐ 50 : 4.965 GHz ☐ 55 : 4.967 GHz ☐ 80 : 4.98 GHz ☐ 20 : 4.95 GHz ☐ 25 : 4.952 GHz ☐ 95 : 4.987 GHz ☐ 90 : 4.985 GHz ☐ 30 : 4.955 GHz ☐ 60 : 4.97 GHz 10MHz Only

Save Cancel

Figure 6-7: Wi-Fi Network (Access Point) Configuration

- c. Configure the AP profile settings based on how they are configured in the actual AP itself. For detailed field information, see [WAN > WiFi Networks > Add New WiFi Network/Configure Network](#) on page 211.
 - d. Click Save.
2. Configure Wi-Fi links to use the AP profile:
 - a. Go to WAN > Links.
 - b. For each Wi-Fi link that will be able to connect to the AP:
 - i. Click Configure in the Actions column for the link.
 - ii. In the list beside the WiFi Networks field, select the AP profile. (Note that a Wi-Fi link can have more than one AP profile selected.)

The screenshot shows the 'WiFi WAN Link Configuration' window. The 'WiFi Networks' section at the bottom has two checkboxes: 'Depot AP' (checked) and 'WiFi network 1' (unchecked). The 'Depot AP' checkbox is circled in red. The window also includes fields for 'Association Settling Period (s)', 'Disassociation Settling Period (s)', 'Background Scanning Interval (s)', 'Signal Strength Average Length', 'Roaming Squelch', 'Minimum Quality of Signal (dB)', 'Satisfactory Quality of Signal (dB)', 'Minimum Quality of Signal Differential (dB)', and 'Permanent Blacklist'. The 'Save' and 'Cancel' buttons are located at the bottom right of the configuration area.

Figure 6-8: Selecting a Wi-Fi AP profile for a Wi-Fi WAN Link

- iii. Click Save.

Note: If multiple Wi-Fi access points are defined, each access point is listed and available for selection in the Wi-Fi link's configuration settings.

6.3 Using Pilot Ping to Pre-test WAN Links

The MG90 can use a 'pilot ping' to determine if a WAN link (Cellular, Ethernet, or Wi-Fi) can pass traffic before the link is identified as established. If pilot ping is enabled and the link cannot pass traffic, it will not be identified as established.

Note: The pilot ping feature for each WAN link is disabled by default, and each link is configured separately.

To enable/disable the pilot ping feature for a Cellular or Ethernet WAN link:

1. Go to WAN > Links.
2. Click Configure in the Actions column for the link.

3. Select Pilot Ping to enable, or deselect to disable the feature. For detailed field information, see [WAN Link Configuration \(WAN > Links > Configure\)](#) on page 170.
4. Click Save.

To enable/disable the pilot ping feature for a Wi-Fi WAN link:

1. Go to WAN > Wi-Fi Networks.
2. Click Configure in the Actions column for the Wi-Fi network that the Wi-Fi WAN link uses.
3. Select Pilot Ping to enable, or deselect to disable the feature. For detailed field information, see [WAN > WiFi Networks > Add New WiFi Network/Configure Network](#) on page 211.
4. Click Save.

6.4 Using WAN Monitors to Detect Lost Connections

The MG90 can use 'monitors' to detect and try to recover from high-level communication failures occurring on a healthy connection between a WAN link and the carrier network. For example, when the MG90 is out of range of the carrier network but the connection is not dropped, the link cannot pass traffic.

A monitor accomplishes failure detection and recovery by periodically checking against its pre-configured parameters for conditions such as a minimum number of connection failures, timeouts, etc.

Tip: *Sierra Wireless strongly recommends that one or more monitors be created and configured for cellular devices.*

Note: Currently, the only supported monitoring method is ICMP ping monitoring.

Creating or modifying monitors

To create or modify a monitor:

1. Go to WAN > Monitors.
2. Click Add New WAN Monitor to create a new monitor, or click Configure in the Actions column to modify an existing monitor.
3. Modify the monitor settings as required to detect a connection that can no longer pass traffic, and ensure the correct Source Address is selected (Monitored Link IP for link monitoring, or the source LAN segment address for VPN monitoring).

For detailed field information, see [WAN > Monitors > Configure](#) on page 200.

4. Click Save.

Enabling monitors on WAN links

To use monitors on a Cellular or Ethernet link, enable them in the link details:

1. Go to WAN > Links.
2. Click Configure in the Actions column for the link.
3. Select the desired monitor(s) in the Monitors list. (Note — More than one monitor can be selected.)
4. Click Save.

To use monitors on a Wi-Fi link, enable them in the Wi-Fi networks (AP profiles) selected in the link:

1. Check which Wi-Fi networks can be used by the Wi-Fi link:
 - a. Go to WAN > Links.
 - b. Click Configure in the Actions column for the Wi-Fi link.
 - c. Make note of the Wi-Fi networks that are selected.

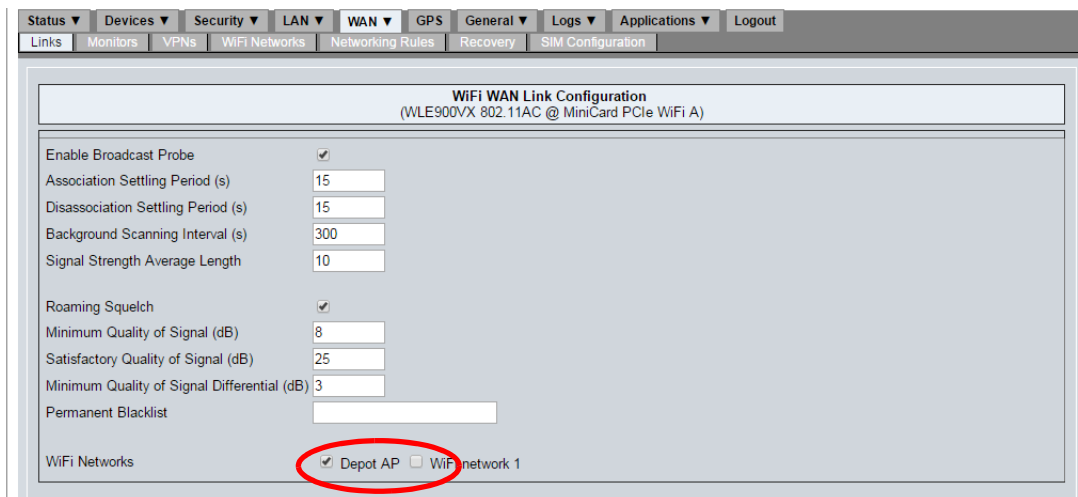


Figure 6-9: Identifying the Wi-Fi networks (AP profiles) selected for a Wi-Fi WAN Link

2. Go to WAN > WiFi Networks.
3. For each Wi-Fi network that will have monitors added:
 - a. Click Configure in the Actions column for the desired network.
 - b. In the Network Settings area, select the desired monitor(s) in the Monitors list. (Note — You can select more than one monitor.)

The screenshot shows the 'WiFi Network Configuration' page. The 'Monitors' checkbox is checked and circled in red, with the 'DefaultMonitor' option selected. Other settings include SSID 'MyWiFi9823', MTU Size '1500', and various IP and DNS configurations.

Figure 6-10: Selecting Monitors for a Wi-Fi Network

- c. Click Save.

Deleting monitors

To delete a monitor:

1. Go to WAN > Monitors.
2. Click Delete in the Actions column for the monitor to delete.
3. Click OK when prompted to confirm the deletion.

6.5 Setting up WAN Link Policies

WAN Link policies are configurable rules that enable the MG90 to choose which WAN links to use at any given time to maintain optimal, cost-effective connectivity across a range of external conditions.

If you have more than one WAN link defined, you may want to define policies to determine which WAN link to use.

Policies determine which link should be used based on a scoring system where:

- Each link starts with a base score of 1000.
- Each link can be individually adjusted by using the Priority Score in the Dynamic Priority Policy screen.

- The link's score may be decreased by defined Penalty values when the link is down, the vehicle's velocity is too high, or the signal strength is too low.
- The link's score may be adjusted by defined amounts when the MG90 is in a certain geographical area, or during specific time periods.
- Each link is evaluated based on its score and the link with the highest score is set to the active link.

Reasons for using link policies include:

- Reducing or eliminating loss of connectivity and associated downtime
- Reducing or eliminating issues associated losing and re-establishing connections, such as having to rebuild a VPN connection
- Maintaining a stable connection
- Maintaining the fastest throughput available
- Reducing cellular usage costs
- Using low-cost links, such as Wi-Fi

The MG90 supports the following link policy types, which you can combine and tune for optimal connectivity and performance:

- Dynamic priority policy — Provides managed switching between WAN links when a link in use goes down. For details, see [Dynamic Priority Policy Overview](#) on page 53.
- Geographic region policy — Defines coverage areas for a WAN link where the link would be the preferred connection device (areas where the device has a strong connection). For details, see [Geographical Regions Policy Overview](#) on page 55.
- Time period policy — Defines times of day when a WAN link should be used (for example, when bandwidth costs are lower, or when network congestion is typically light). For details, see [Time Period Policy Overview](#) on page 57.
- Velocity policy — Defines a maximum vehicle speed for a WAN link to be used (for example, to use a Wi-Fi WAN link only when at its depot, traveling in the yard at low speed). For details, see [Velocity Policy Overview](#) on page 57.
- Signal strength policy — Defines the minimum preferred RF signal conditions for a WAN link (for example, to use a Wi-Fi link only when it has a strong enough signal). For details, see [Signal Strength Policy Overview](#) on page 58.

Defining WAN link policies

To define policies for a WAN link:

1. Go to WAN > Links.
2. Click Policies in the Actions column for the link.
3. Click Configure in the Actions column for a desired policy type.
4. Select Enable this policy.
5. Configure the policy settings. For detailed field information for each policy type, see [WAN Link Policy Configuration \(WAN> Links > Policies\)](#) on page 190.
6. Click Save.

When the WAN Link Policy Configuration screen redisplay, you will see the policy's Enabled checkbox is selected.

7. Repeat for any additional policies that should be configured.

Note: Policy configurations are unique for each link, and must be configured on a per link basis as required. For example, if you have Velocity policies on two Wi-Fi WAN links, they are configured separately, even if they are set up with identical details.

6.5.1 Special Considerations for Wi-Fi Links

When planning how policies will be used to select/deselect Wi-Fi links, remember to consider the Association Settling Period and Disassociation Settling Period values for each Wi-Fi link (see [Wi-Fi WAN Link Configuration](#) on page 184 for a description of these settings).

These settings prevent accidental selection and deselection of a Wi-Fi link which could occur when brief Wi-Fi connectivity is available (e.g. when driving past a depot's Wi-Fi hotspot).

Note: These settings are not available on cellular devices.

By default, these values default to 15 seconds, and will prevent a Wi-Fi link's status from changing from "DOWN" to "UP" (Association Settling Period) or "UP" to "DOWN" (Disassociation Settling Period). This makes the link unavailable for selection by a policy during the settling period time frame.

As a result, penalties and recovery periods of policies on Wi-Fi links can generally be set to 0, since the two settling periods already handle most situations where brief Wi-Fi connectivity is to be ignored.

6.5.2 Dynamic Priority Policy Overview

The Dynamic Priority Policy is intended for use when an MG90 has multiple WAN devices that can provide backup connections when the active link in use goes down.

The policy provides a managed switch between WAN links, where the next-best link is used until the link that went down reconnects and maintains a stable connection for a defined recovery period (long enough to prove that it is 'trustworthy'). This prevents the active link from switching back and forth to an unstable link (a link that quickly and repeatedly goes up and down).

The Dynamic Priority Policy Configuration screen includes two groups of settings:

- Priority score — When enabled, the Priority Score adjustment is added to the link's base score of 1000. Use this to indicate the relative priority of each WAN link. (Note that you can assign the same priority to more than one link if they are equally preferable.)

Important: *Although this setting appears on the configuration screen of the Dynamic Priority Policy, it is not specific to that policy and can be set and used with any policy.*

- Dynamic priority policy — If enabled, a link's score automatically decreases by the Link Down Penalty value when the link goes down (e.g. when it loses its connection). When the link comes back up, it 'proves' its stability over the Recovery Period during which the penalty is gradually reduced. By tuning the Penalty and Recovery Period values, you can ensure a link is only used when it has a stable connection.

For example, if a link has a score of 1200 when it goes down and has a Link Down Penalty of 120:

- The link's score immediately drops to 1080 (1200 - 120).
- If the Recovery Period is:
 - 0 seconds — The link's score immediately returns to 1200 when the link comes back up.
 - 60 seconds — The link's score increases by 2 points per second when the link comes back up (120 point penalty / 60 seconds).

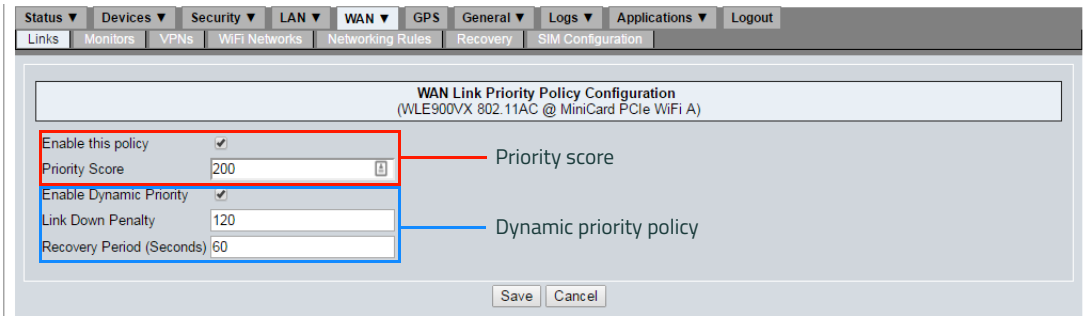


Figure 6-11: Dynamic Priority Policy—Example

6.5.2.1 Dynamic Priority Policy Example

In this example, a vehicle carries an MG90 that has three WAN links — two LTE radios (CA and CB) and a Wi-Fi radio. The Wi-Fi radio is the most preferred device, followed by CA and then CB. To model this in the Dynamic Priority policy the following settings were used:

Table 6-1: Example of Dynamic Priority Settings

	Wi-Fi	CA	CB
Base Score	1000	1000	1000
Priority Score	300	200	100
Link Down Penalty	Not Enabled	300	300
Recovery Period	Not Enabled	120	120

Figure 6-12 is a simple time line showing the dynamic priority policy affecting the WAN link scores:

- T_1 — Vehicle is not near a depot; CA (score = 1200) is the current WAN link.
- T_2 — CA connection is lost. CA's score is re-calculated ($1200 - \text{Penalty}(300) = 900$). CB has a higher score (1100), so CB becomes the current WAN link.
- T_3 — CA re-establishes connection and begins its 120 second recover period, increasing its score by $300/120$ points per second. CB is still the current WAN link.
- T_4 — CA score has increased and is now higher than CB's score. CA is restored as the current WAN link (and continues to increase its score while it is still in the recovery period).
- T_5 — CA score is now back to normal (1200).
- T_6 — Vehicle enters the Wi-Fi zone of a depot. Wi-Fi has a higher score (1300), so Wi-Fi becomes the active link.

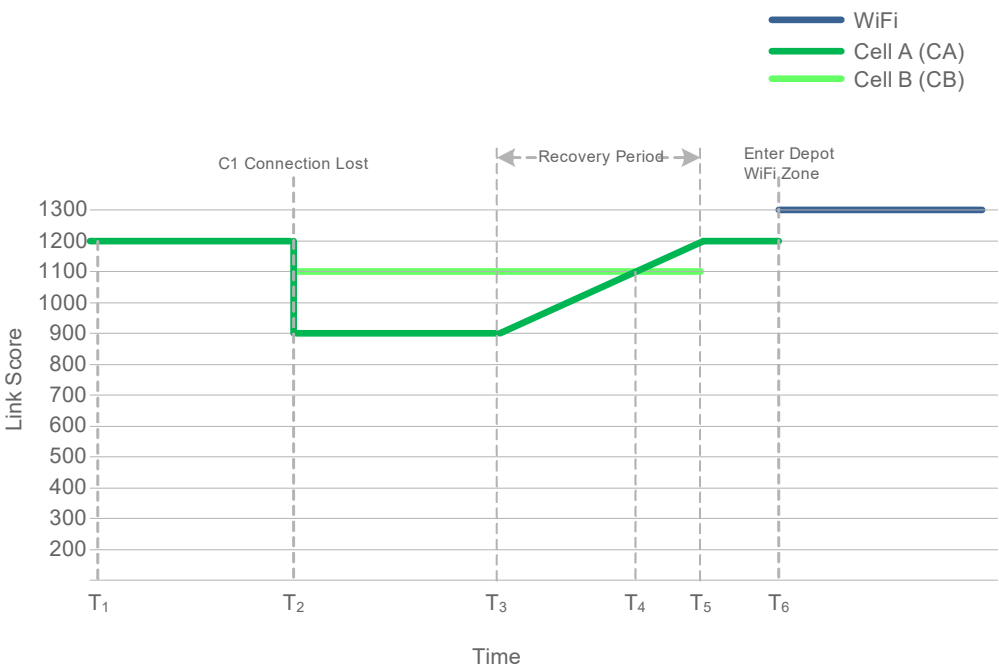


Figure 6-12: Dynamic Priority Timeline—Example

Note: [Figure 6-12](#) provides a basic introduction to how policies use scoring to switch between links. In practice, other factors (such as a Wi-Fi device's Association Settling Period) mean that switches won't happen instantaneously.

Tip: A priority score of 100 with a penalty of 300 and a 120 second recovery time, make for good, “granular” numbers to use because they make it easy to monitor switchovers (e.g. via logging) when using the Dynamic Priority policy. In particular, a 120 second recovery time allows for a ping monitor to occur every 30 seconds so that three pings occur during the recovery period.

For detailed field information, see [Table E-7, WAN > Links > Policies > Configure \(Dynamic\) screen fields](#), on page 191.

6.5.3 Geographical Regions Policy Overview

The Geographical Regions Policy is used to increase a WAN link’s score in up to three geographic areas (rectangular) to make it the preferred link in those areas.

This policy is often used when the quality and/or cost of coverage for particular areas is known and not likely to change.

For example:

- If the cellular coverage for different carriers is known to be good in certain areas, then regions for those areas can be defined on the respective WAN links and scores applied accordingly.
- If a Wi-Fi connection is available (e.g. in and around a depot), then a region for the depot could be defined for the Wi-Fi WAN link with a very high score to ensure the Wi-Fi WAN link is used when the vehicle is in or near the yard.

6.5.3.1 Geographical Regions Policy Example

In this example, a vehicle carries an MG90 with two cellular WAN links (LTE radios — CA and CB) and operates in an area ([Figure 6-13](#) on page 57) where:

- CA has the best coverage in one region (Region 1)
- CB has the best coverage in another region (Region 2)
- The coverage areas for CA and CB overlap. In the overlap area, CA is preferred over CB.

To provide the best coverage and prevent unnecessary switchovers throughout the vehicle's journey, the following policy settings were used:

Table 6-2: Example of Geographical Regions Policy Settings

Cellular WAN Link	Dynamic Priority Policy	Geographic Region Policy
CA	Priority (Base) Score: 1200	Region 1 Score: 300 Region 2 Score: 0
CB	Priority (Base) Score: 1100	Region 1 Score: 100 Region 2 Score: 300

The overall score for a cellular link is then calculated as follows:

- Single region: Overall score = Priority Score + Score for current region
- Overlapping regions: Overall score = Priority Score + Score for first overlapped region + Score for second overlapped region + ...

For example, when the vehicle is in:

- Region 1:
 - CA score = $1200 + 300 = 1500$
 - CB score = $1100 + 100 = 1200$
 - CA will be used (if available) when the vehicle is fully in Region 1.
- Region 2:
 - CA score = $1200 + 0 = 1200$
 - CB score = $1100 + 300 = 1400$
 - CB will be used (if available) when the vehicle is fully in Region 2.
- Overlap (Region 1 and Region 2):
 - CA score = $1200 + 300 + 0 = 1500$
 - CB score = $1100 + 100 + 300 = 1500$
 - CA and CB are equally preferable. As shown in [Figure 6-13](#), when the vehicle moves from one region into the overlapping zone, a switch between cellular links will not occur.

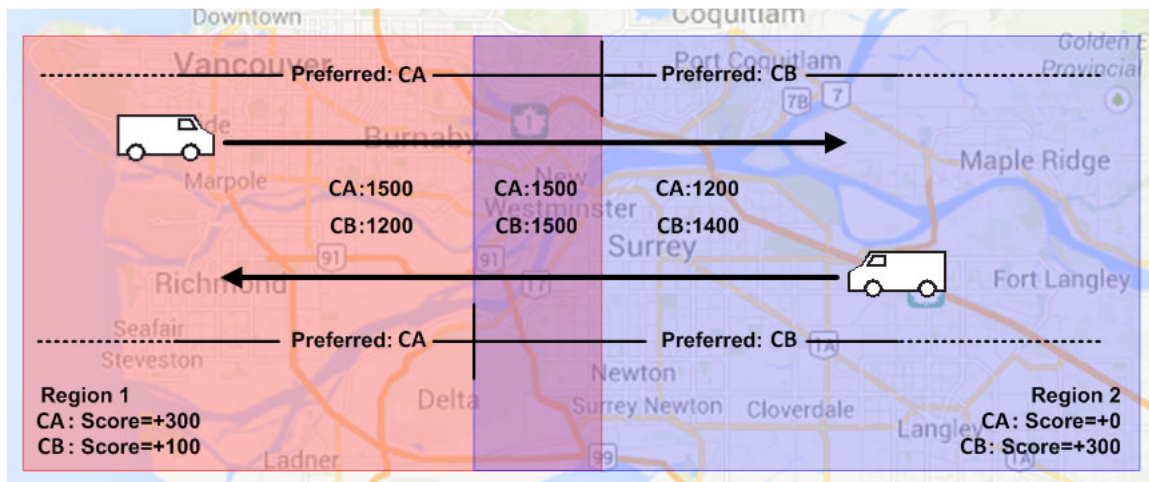


Figure 6-13: Geographical Regions Example with Overlapping Regions

Note: Region boundaries are defined using latitude and longitude coordinates. You must determine and manually enter these coordinates—the MG90's LCI does not provide a mapping interface to visually define zones.

For detailed field information, see [Table E-8, WAN > Links > Policies > Configure \(Geographical\) screen fields](#), on page 193.

6.5.4 Time Period Policy Overview

The Time Period Policy is used to increase a WAN link's score during defined time periods (up to three periods per link) to make it the preferred link during those periods.

This policy is typically used to take advantage of reduced data costs or to compensate for bandwidth saturation periods. For example:

- If a normally preferred WAN link's throughput is known to drop during a particular time of day (e.g. due to network congestion), define a time period policy with a high score on a different WAN link to temporarily use that link and maintain acceptable throughput.
- If a carrier provides cheaper cellular coverage during evenings, define a time period policy for that WAN link.

For detailed field information, see [Table E-9, WAN > Links > Policies > Configure \(Time Period\) screen fields](#), on page 194.

6.5.5 Velocity Policy Overview

The Velocity Policy is used to decrease a WAN link's score when the vehicle exceeds a maximum velocity.

This policy is typically used when a Wi-Fi WAN link is used at a depot that has Wi-Fi coverage in the depot area and in a small zone outside of the depot. When the vehicle travels inside the depot, it travels at low speed (for example, a maximum of 20 mph). When it leaves the depot and begins to pass out of the coverage zone, it increases its speed.

If a velocity policy is defined with an appropriate speed threshold, the current WAN link will switch seamlessly from the Wi-Fi link to (for example) a cellular WAN link without a drop in connection, preventing issues such as having to rebuild a VPN connection which would occur if the Wi-Fi link dropped without switching to the cellular link.

For example (as shown in [Figure 6-14](#)), a velocity policy could be set with a 20 mph threshold. When the vehicle leaves the depot and begins accelerating, it switches over to a cellular WAN link before it reaches the edge of the Wi-Fi coverage area.

If the vehicle re-enters the Wi-Fi coverage area at a speed lower than the maximum, the Wi-Fi WAN link ‘proves’ its stability over the Recovery Period during which the penalty is gradually reduced. By tuning the Penalty and Recovery Period values, you can ensure a link is only used when the vehicle appears to be staying in the coverage area (rather than simply passing through).

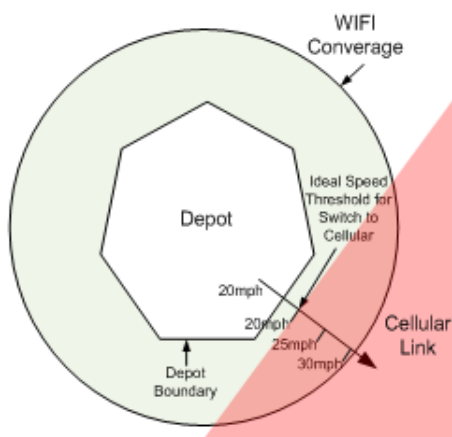


Figure 6-14: Setting a Speed Threshold to Switch to Cellular before Wi-Fi Coverage is lost

Note: GPS “jitter” can occur when the vehicle is parked or the GPS signal is weak (such as when indoors or in a covered area), which can cause the speed threshold(s) defined in the Velocity Policy to be satisfied, resulting in an inadvertent switch in links. Sierra Wireless recommends that a GPS repeater be installed near the depot to reduce GPS jitter. Also, a GPS jitter filter can optionally be enabled (see [GPS Configuration Set Up](#) on page 95) to ignore small reported movements (not suitable for high-sensitivity reporting requirements).

For detailed field information, see [Table E-10, WAN > Links > Policies > Configure \(Velocity\) screen fields](#), on page 195.

6.5.6 Signal Strength Policy Overview

The Signal Strength Policy is used to decrease a cellular or Wi-Fi WAN link’s score when the connection’s signal strength (RSSI) and other optional RF condition metrics (RSRP, RSRQ, SINR) fall below minimum user-configurable thresholds, which makes other WAN links with stronger signals more preferable.

When the applicable metrics rise back above their respective thresholds, they ‘prove’ their stability over the Recovery Period. If the metrics remain above the thresholds for the entire Recovery Period, the penalty is removed. By tuning the Penalty and Recovery Period values, you can ensure the link has a strong and stable signal before switching back to it.

When setting the RF metrics thresholds for the WAN links:

- If a specific WAN link is generally preferred (e.g. due to lower data plan costs), then the Signal Strength Policy for that link should indicate lower thresholds (lower quality) than the policies on the other links. This will help ensure that the preferred link is utilized the most as RF conditions between devices fluctuate.
- If multiple WAN links are equally preferable, the thresholds in the Signal Strength Policies for each link should be set the same. This will prevent unnecessary switchovers from occurring since both devices are designated as equally capable.

Important: The default thresholds for each RF metric are typically sufficient to drop bad connections that may not cause ping monitor failures.

Table 6-3 describes general signal quality ranges for each metric:

Table 6-3: Signal Quality Indicators^a

RF Condition	RSSI (dBm)	RSRP (dBm) 5G RSRP (dBm)	RSRQ (dB) 5G RSRQ (dB)	SINR (dB) 5G SINR (dB)
Excellent	≥ -70	≥ -80	≥ -10	≥ 20
Good	-70 to -85 ^b	-80 to -90	-10 to -15	13 to 20
Fair	-86 to -100	-90 to -100 ^b	-15 to -20 ^b	0 ^b to 13
Poor	≤ -100	$\phi \leq -100$	≤ -20	≤ 0

a. RSRP, RSRQ, and SINR (and 5G equivalents) are useful indicators for LTE and 5G.

b. MG90 default threshold for the indicated RF metric

For detailed field information, see [Table E-11, WAN > Links > Policies > Configure \(Signal Strength\) screen fields](#), on page 196.

6.5.6.1 Signal Strength Policy Examples

Figure 6-15 illustrates how the signal strength policy is applied when all metrics must be below their respective thresholds, and when any metric is below its threshold.

In these examples:

- A vehicle carries an MG90 with two cellular WAN links (LTE radios — Link A and Link B).
- The base score for Link A is higher than the base score for Link B. When no penalty is assessed, Link A is the primary.
- Only Link A has any policies enabled (Signal Strength policy only)
- All RF metrics are enabled with thresholds set to default values.
- Signal sample size is 5 (i.e., 10 s rolling sample window)

In the first example, a penalty is applied when the average samples for all metrics drop below their thresholds and Link B becomes the primary. The penalty is removed when all the average samples for all metrics rise back above their thresholds and Link A becomes the primary.

In the second example, a penalty is applied when the average samples for RSSI and RSRP both drop below their respective thresholds and Link B becomes the primary. While the penalty is in force, the other metrics also drop below their respective thresholds. The penalty is removed when all the average samples for all metrics rise back above their thresholds and Link A becomes the primary.

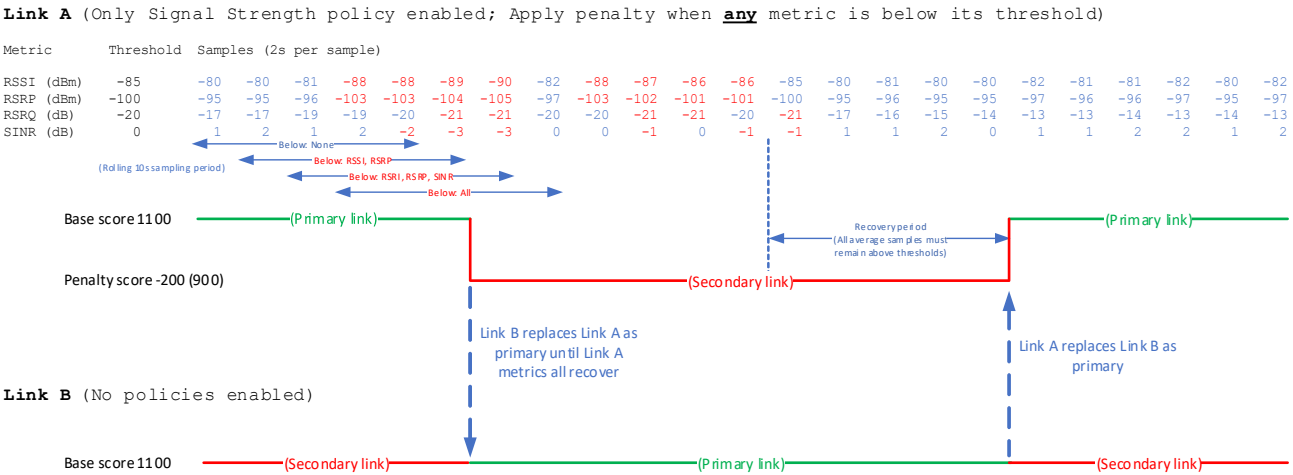
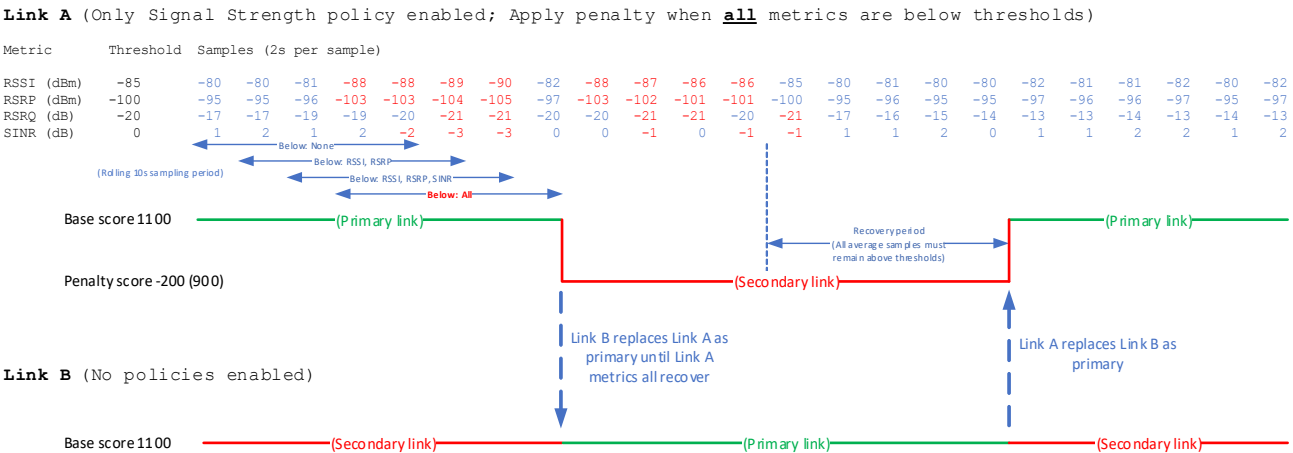


Figure 6-15: Signal Strength Policy Examples

6.5.7 Use Cases

6.5.7.1 Dynamic Priority Policy and Velocity Policy Combination

The following example shows how to combine the Dynamic Priority Policy with the Velocity Policy to choose between links.

In this example, an MG90 has two WAN links enabled — a Wi-Fi link and a cellular link. The user wanted to use the depot Wi-Fi link whenever possible since the Wi-Fi link has superior performance, connection quality, and lower usage costs than the cellular link.

To model this, Dynamic Priority and Velocity policies were configured for the Wi-Fi WAN link with the following settings (no policies were created for the Cellular link):

Table 6-4: Example WAN Link Policy Settings for Use Case

	Cellular	Wi-Fi	Effect
Priority Base Score (Not adjustable)			
Base Score	1000	1000	All links have the same base score.
Dynamic Priority Policy			
Priority Score	No policy	200	Wi-Fi (the preferred link) priority (before any penalties) increases to 1200.
Link Down Penalty		600	When Wi-Fi link is lost (e.g. when out of range of depot access point), score decreases by 600 points.
Recovery Period		780 seconds	When Wi-Fi link comes back up, the penalty recovers linearly (score increases) by 600/780 points/second.
Velocity Policy			
Threshold	No policy	25 mph	Depot has 25 mph speed limit. Vehicle speed > 25 mph implies the vehicle has left the depot and will soon be out of Wi-Fi range.
Penalty		400	Wi-Fi link score decreases by 600 points when vehicle exceeds the threshold.
Recovery period		240 seconds	When vehicle speed decreases to ≤ 25 mph, the penalty decreases by (400/240 points/second). This ensures the link doesn't immediately switch, while the vehicle 'proves' it is staying in the coverage area rather than passing through.

Figure 6-16 is a simple timeline showing how the MG90 uses this configuration to choose between its WAN links (Wi-Fi and cellular).

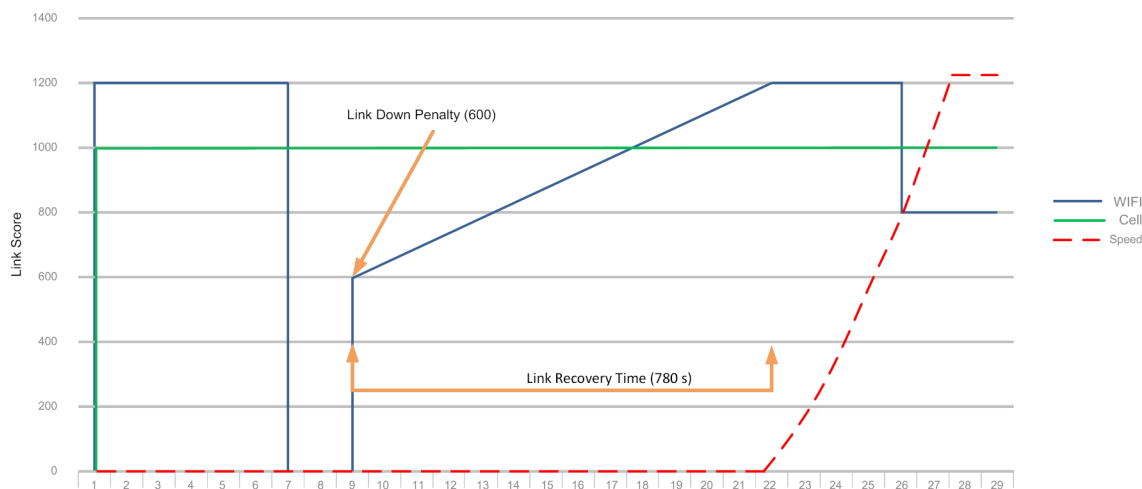


Figure 6-16: Dynamic Priority and Velocity Policy Combination

The following can be observed on this timeline:

- Wi-Fi starts with a higher score of 1200; cellular with 1000. The vehicle is stationary (speed is 0 mph).
- At 7 minutes, the Wi-Fi connection is lost and the cellular connection takes over.

- At 9 minutes, the Wi-Fi link recovers and the Dynamic Priority Policy sets its score to 600 (1200 - 600 penalty), which is lower than the cellular link's score (1000). The Wi-Fi link's score increases over its link recovery period at a rate of 0.77 points per second (600 point penalty recovered over 13 minutes).
- At 18 minutes:
 - The Wi-Fi link's score has recovered enough to exceed the cellular link's score, and the Wi-Fi link becomes the active link again.
- At 22 minutes:
 - The vehicle starts to accelerate.
- At 26 minutes, the vehicle's speed exceeds the speed threshold defined in the Velocity Policy on the Wi-Fi link. The Wi-Fi link's score drops by 400 points (velocity penalty) causing the cellular link to take over.

6.6 Setting up the WAN Firewall

6.6.1 Configuring WAN Networking Rule Firewall Settings

WAN firewall settings are configured by creating WAN networking rules.

The MG90's WAN firewall can deny/allow access to incoming and outgoing traffic based on a source/destination IP address combination, using TCP, UDP, or both protocols. The firewall also supports port forwarding so services within the MG90's LAN may be accessible over the WAN.

Note: There are three 'levels' of networking rules — LAN segment, WAN link, and Global (LAN). If there is a conflict between any of these rules, LAN segment rules override WAN link and global rules, and WAN link rules override global rules.

6.6.1.1 Defining WAN Firewall Rules

To define WAN firewall rules:

1. Go to WAN > Networking Rules.
2. Select the rule type in the drop-down (Access Blocking, Access Granting, or Port Forwarding).
3. Click Add New Networking Rule.
4. Enter a descriptive name for the rule in the Rule Name field.
5. Select the traffic Direction affected by the rule.
6. Configure the remaining fields. For detailed field information for each rule type, see [WAN > Networking Rules](#) on page 220.
7. Click Save.

Note: You can combine Access Blocking and Access Granting rules to implement very specific access policies. Multiple rules of each type may also be created.

6.6.1.2 Deleting WAN Firewall Rules

To delete a WAN firewall rule:

1. Go to WAN > Networking Rules.
2. Click Delete in the Actions column for the desired rule.

3. Click OK when prompted to confirm the deletion.

6.7 WAN Link Recovery

The MG90 can be configured to reboot after WAN connectivity has been down for a specified amount of time.

To enable WAN recovery:

1. Go to WAN > Recovery.
2. Select WAN Link Recovery.
3. Configure each recovery setting as required. For detailed field information, see [WAN > Recovery](#) on page 228.
 - WAN Link Recovery — If enabled, forces the MG90 to reboot (after specified time) if WAN connectivity is lost.
 - Remote Configuration WAN Recovery — If enabled, restores the previous configuration (after specified time) when changes that were made remotely on an AMM caused a loss of WAN connectivity.
4. Click Save.

In addition to using the WAN recovery feature, the Pilot Ping option for Cellular, Ethernet, and Wi-Fi WAN link options can be used to determine if a WAN link can pass traffic before the link is identified as established, and ping Monitors can attempt to restart a failed WAN link. See field listings in [WAN Link Configuration \(WAN > Links > Configure\)](#) on page 170. (for Pilot Ping and Monitors), and [Using WAN Monitors to Detect Lost Connections](#) on page 49.

7: Setting up the LAN

The MG90 provides LAN access using two methods:

- **Wired**— Access via Ethernet ports 1–5. By default, ports 1–4 are configured for LAN, and port 5 is configured for WAN. To assign Ethernet ports for LAN use, see [Configuring Ethernet Ports](#) on page 24.
- **Wireless**— Access via Wi-Fi Access Points (AP). (Each Wi-Fi radio can be used as a unique access point.) To assign Wi-Fi devices for LAN use, see [Configuring Wi-Fi Devices](#) on page 24.

Note: The MG90 does not support USB-to-Ethernet adapters for LAN operation.

Before deploying the MG90, make sure to configure the LAN links with appropriate security and settings. The following topics describe typical setup requirements:

- [Ethernet LAN Link Configuration](#) on page 64
- [LAN Access Point Configuration](#) on page 65
- [Configuring LAN Segments](#) on page 65
- [Configuring DHCP and Static IP Addresses](#) on page 68
- [Setting up the LAN Firewall](#) on page 69
- [Setting up Virtual LANs](#) on page 69
- [Setting up Captive Portals](#) on page 70

7.1 Ethernet LAN Link Configuration

Note: LAN configuration of each Ethernet port can be set regardless of its current use (WAN, LAN, IDLE).

To configure Ethernet ports for LAN access:

1. Go to LAN > Ethernet Links.

Device Type	Friendly Name	Configure
Device Built-in Ethernet Port	Panel Ethernet 1	Configure
Device Built-in Ethernet Port	Panel Ethernet 2	Configure
Device Built-in Ethernet Port	Panel Ethernet 3	Configure
Device Built-in Ethernet Port	Panel Ethernet 5	Configure

Figure 7-1: LCI: LAN > Ethernet Links

2. Enable (or disable) 802.1x network access control for a specific Ethernet port. (Note: If you disable network access control, any device that connects to the port can access the network.):
 - a. Click [Configure](#) for the desired Ethernet port.
 - b. Select **Enable wired 802.1x network access control** to display the configuration fields (or deselect the checkbox to disable network access control).
 - c. Configure the 802.1x settings. For detailed field information, see [LAN Ethernet Configuration \(LAN > Ethernet Links > Configure\)](#) on page 141.
 - d. Click **Save**.

7.2 LAN Access Point Configuration

Note: LAN configuration of each Wi-Fi device can be set regardless of its current use (WAN, LAN, IDLE).

To configure LAN access points (maximum one AP for each Wi-Fi radio in the MG90):

1. Go to LAN > Access Points.
2. Click Configure in the Actions column for the desired device.
3. Configure the access point settings. For detailed field information, see [Access Point Configuration \(LAN > Access Points > Configure\)](#) on page 144.

Note: Each access point can be enabled/disabled as required. Disabling a configured access point does not affect the configuration options, it only prevents the access point from being used.

4. Click Save.

7.3 Configuring LAN Segments

LAN segmentation, and the process of adding LAN segments, is used for advanced networking scenarios when LAN traffic from different devices must be partitioned.

For example, LAN segmentation can be used when public Internet access is made available for Wi-Fi users while private onboard equipment connected to the MG90's Ethernet ports must not be accessible by Wi-Fi users. Multiple LAN segments are useful for specifying different network policies or routing rules on each segment.

By default, the MG90 is pre-configured with one LAN segment ("Default LAN") on which all factory-enabled LAN links operate:

- Ethernet links — Can be assigned to one segment only
- Wi-Fi links — Can be assigned to multiple segments when configured with up to three additional BSSIDs. For example, a Wi-Fi link with one additional BSSID can be assigned to two segments.

Before deploying an MG90, it's important to review how the LAN segment(s) are configured on the unit to ensure that network traffic visibility remains as secure as possible.

7.3.1 Add/Configure LAN Segments

By default, the MG90 includes one LAN Segment — Default LAN, and all LAN-capable devices are assigned to that segment.

Note: A Serial LAN segment will appear in the list if the MG90's serial port is configured for LAN use (Devices > Serial). This segment is automatically created when the serial port is configured as LAN, and automatically deleted if port is reconfigured for Application or Console use.

To add or configure LAN segments:

1. Go to LAN > LAN Segments.

Subnet	Friendly Name	Devices	Type	Enabled	Actions
172.22.0.0/24	Default LAN				Configure Networking Rules
		• ND605118181818: WLE900VX 802.11AC @ MiniCard PCIe WiFi A	WiFi	☐	Default LAN ▼
		• ND605118181818: WLE900VX 802.11AC @ MiniCard PCIe WiFi B	WiFi	☒	Default LAN ▼
		• Panel Ethernet 1	Ethernet	☐	Default LAN ▼
		• VID 1313: Rear Panel Ethernet Ports	VLAN	☒	Default LAN ▼
		• VID 1492: Rear Panel Ethernet Ports	VLAN	☒	Default LAN ▼
		• VID 1999: Rear Panel Ethernet Ports	VLAN	☒	Default LAN ▼
		• VID 1234: Rear Panel Ethernet Ports	VLAN	☒	Default LAN ▼
		• VID 2400: Rear Panel Ethernet Ports	VLAN	☒	Default LAN ▼
		• Panel Ethernet 4	Ethernet	☒	Default LAN ▼
		• Panel Ethernet 5	Ethernet	☐	Default LAN ▼
172.22.1.0/24	TEST LAN-1				Delete Configure Networking Rules
172.22.2.0/24	LAN-1				Delete Configure Networking Rules
172.22.1.0/24	Serial LAN				Configure Networking Rules
		• Panel RS-232 Serial	Serial	☒	Serial LAN ▼

Figure 7-2: Configuring or adding a LAN segment

- If you want to:
 - Add a new LAN segment — Click Add New LAN Segment.
 - Modify an existing LAN segment — Click Configure in the Actions column for the desired segment.
- Configure the segment's settings. For detailed field information, see [LAN Segment Configuration \(LAN > LAN Segments > Configure\)](#) on page 154.

LAN Segment Configuration
(Default LAN)

Friendly Name:

Default Gateway Address:

Network Mask:

Enable DHCP Server: ☒

DHCP Low Address:

DHCP High Address:

DHCP Client Lease Time (sec):

Domain search list (comma-separated):

WINS Servers (comma-separated IP addresses):

Enable Web Portal: ☐

Enable Subnet Management Access: ☒

Enable Subnet SSH Shell Access: ☐

Isolated: ☐

IGMP Snooping: ☐

IPv6 Addressing:

Figure 7-3: Standard LAN Segment Configuration screen

LAN Segment Configuration
(Serial LAN)

Friendly Name:

Default Gateway Address:

Peer Address:

Figure 7-4: Serial LAN LAN Segment Configuration screen

4. Click Save.

Note: Each LAN segment must have a different scope (i.e. IP address range or network mask) from the other segments. A warning appears if an attempt is made to cross segment scopes, as shown in Figure 7-5:

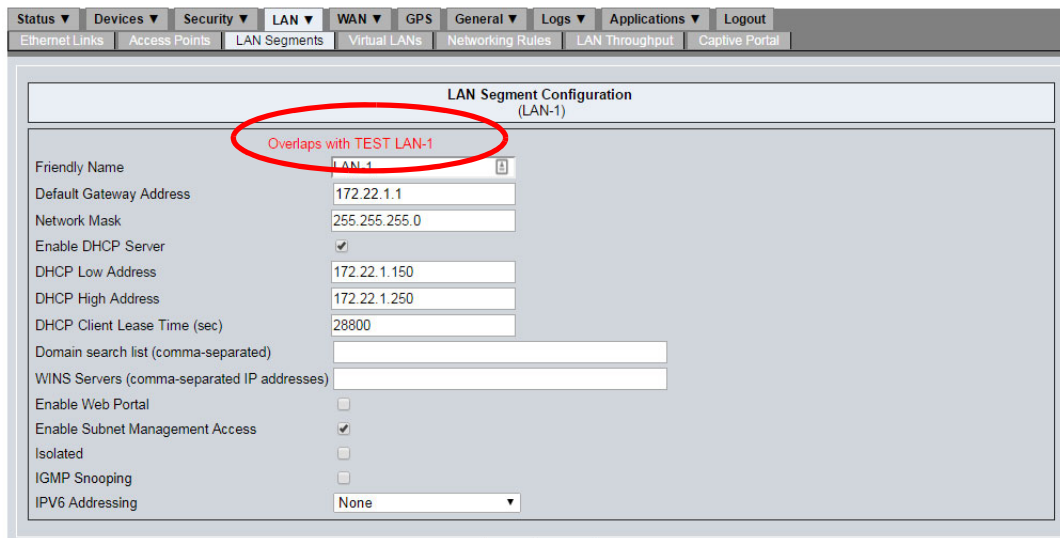


Figure 7-5: Warning for a segment configuration address range which overlaps another

7.3.2 Assign a Device to a Different LAN Segment

To assign a device to a different LAN segment:

1. Go to LAN > LAN Segments.
2. Locate the device you want to reassign, then select the desired LAN segment from the drop-down in the device's Actions.
3. Click Apply Changes. The screen will refresh and the device listing now appears in the LAN Segment you selected.

7.3.3 Delete a LAN Segment

If required, you can delete any of the LAN segments that you created (the Default LAN cannot be deleted). This can only be done if there are no devices on the segment (the Delete option will not appear on a segment that is in use).

To delete a LAN segment:

1. Go to LAN > LAN Segments.
2. Click Delete in the Actions column for the segment.
3. Click OK when prompted to confirm the deletion.

When a segment is deleted, the interface(s) that were assigned to it are reassigned to the Default LAN segment.

Note: The Serial LAN segment (if present) can only be deleted by changing the Serial port's use to Application or Console (in Devices > Serial).

7.4 Configuring DHCP and Static IP Addresses

Each LAN segment (except the Serial LAN segment) can be configured to assign IP addresses to LAN devices using DHCP, or can utilize statically assigned IP addresses.

LAN segment default settings:

- Default LAN segment:
 - DHCP address range: 172.22.0.100–172.22.0.200
 - Router address: 172.22.0.1
- Default additional LAN segments:
 - DHCP address range: 172.22.x.100–172.22.x.200
 - Router address: 172.22.x.1

The 'x' value increments from the previous segment. For example, the first additional segment would use '1', the second would use '2', etc.

Note: The settings noted above are default settings. These can be modified as necessary.

To configure the IP addresses for a LAN segment:

1. Go to LAN > LAN Segments.
2. Click Configure in the Actions column for the segment.
3. Set the desired address assignment method (DHCP or Static IP) as follows (for detailed field information, see [LAN Segment Configuration \(LAN > LAN Segments > Configure\)](#) on page 154):
 - To use DHCP:
 - i. Select Enable DHCP Server.
 - ii. Assign the DHCP address range and lease time in the DHCP Low Address, DHCP High Address, and DHCP Client Lease Time fields.
 - To use static IP addresses:
 - i. De-select Enable DHCP Server.
 - ii. Ensure each device on the segment has been configured with a unique static IP address (using the configuration tools available on each device).
4. Click Save.

7.5 Configuring the Serial LAN Segment

The Serial LAN segment is automatically created when the MG90's serial port is configured for LAN use (Devices > Serial); it cannot be created from LAN > LAN Segments. (To create the Serial LAN segment, see [Configuring the Serial Port](#) on page 25.)

This configuration connects the serial port to a Sierra Wireless GNX AirLink Companion device, allowing the device to transfer vehicle telemetry data over the MG90's WAN connection instead of using its own cellular radio module.

If the default Serial LAN configurations conflicts with other LAN segments, configure the Serial LAN segment as follows:

1. Go to LAN > LAN Segments.
2. Click Configure in the Actions column for the Serial LAN segment.
3. Set the Default Gateway Address (address assigned to the MG90 serial interface).

4. Set the Peer Address (address assigned to the client, in the Default Gateway Address's subnet).
5. Click Save.

7.6 Setting up the LAN Firewall

7.6.1 Configuring LAN Networking Rule Firewall Settings

LAN firewall settings are configured by creating LAN networking rules.

The MG90's LAN firewall can deny/allow access to incoming and outgoing traffic based on a source/destination IP address combination, using TCP, UDP, or both protocols.

Note: There are three 'levels' of networking rules — LAN segment, WAN link, and Global (LAN). If there is a conflict between any of these rules, LAN segment rules override WAN link and global rules, and WAN link rules override global rules.

7.6.2 Defining LAN Firewall Rules

To define LAN firewall rules on the MG90:

1. Go to LAN > Networking Rules.
2. Select the rule type in the drop-down (Access Blocking, Access Granting, or QoS Prioritizing).
3. Click Add New Networking Rule.
4. Enter a descriptive name for the rule in the Rule Name field.
5. Select the traffic Direction affected by the rule.
6. Configure the remaining fields. For detailed field information for each rule type, see [LAN > Networking Rules](#), and [LAN > LAN Segments > Networking Rules](#) on page 158.
7. Click Save.

Note: You can combine Access Blocking and Access Granting rules to implement very specific access policies. Multiple rules of each type may also be created.

7.6.3 Deleting LAN Firewall Rules

To delete a LAN firewall rule:

1. Go to LAN > Networking Rules.
2. Click Delete in the Actions column for the desired rule.
3. Click OK when prompted to confirm the deletion.

7.7 Setting up Virtual LANs

Virtual LANs (VLAN) can be used when devices inside the vehicle require VLAN tagging for their operation, or when the vehicle LAN has a switch with VLAN tagging enabled. If a vehicle has VLANs configured, or requires additional Ethernet ports, they can be added by using a switch and VLAN tagging.

For information on VLAN configuration settings, see [VLAN Configuration \(LAN > Virtual LANs\)](#) on page 156.

7.8 Setting up Captive Portals

The MG90 supports the use of Captive Portals to control access to specific Wi-Fi networks.

When a user connects to a captive portal to access a Wi-Fi network, they may have to identify themselves, agree to an acceptable use policy, and arrange payment for fee-based services if available (for example, paying for premium services (higher speeds, access to certain websites or content, etc.).

Captive portals can be managed either by external portal servers (providing the full range of captive portal functionality), or by the MG90 via its built-in 'miniportal' that provides a more limited range of features. Some features that captive portals can provide include:

- General access to free Wi-Fi without requiring user authorization
- Limiting access to authorized users (sign-in required)
- Per user directed marketing
- Per user quota management
- Traffic shaping/bandwidth throttling
- Fee based services
- Content filtering to block inappropriate content

[Figure 7-6](#) on page 71 shows a basic overview of how the captive portal feature works, with references to settings in [LAN > Captive Portal > Configure](#) on page 165.

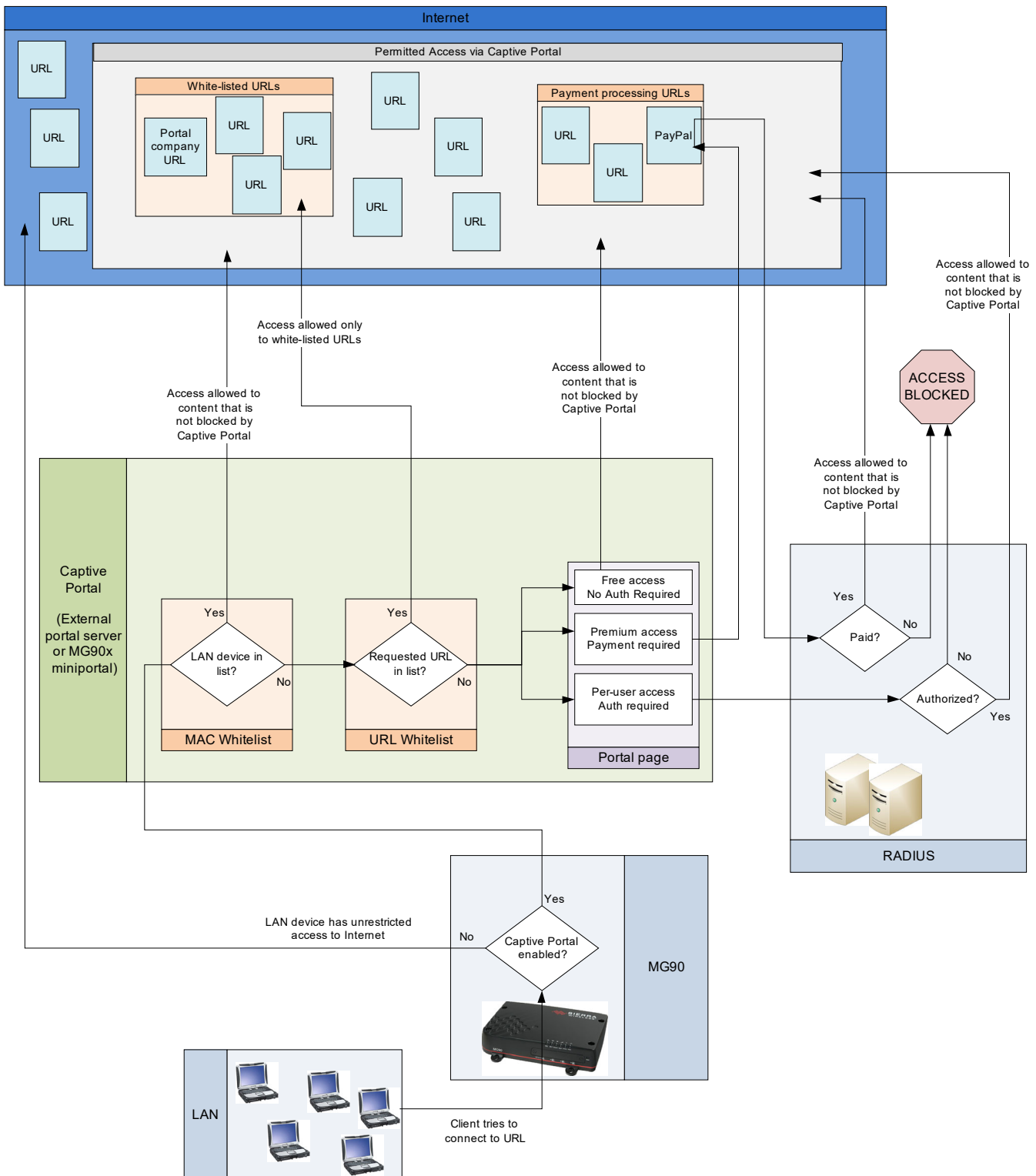
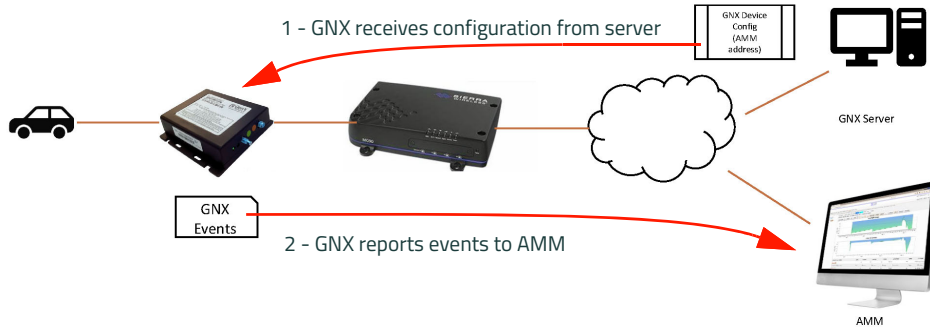


Figure 7-6: Captive Portal Overview

8: Supporting Connection From GNX AirLink Companion Device

The AirLink MG90 can act as a connection gateway for a GNX AirLink Companion device, allowing the GNX device to use the MG90's WAN connection (via the MG90's GNX Companion Application) instead of its own modem or other external modems.



The GNX Companion device uses this connection to report data to AMM (the AMM address is stored in the GNX device's configuration). For detailed information about the GNX Companion device, including server and device configuration, refer to the GenX Reference Guide ([2] Gen-X Mobile Tracker — GNX20/6/5P/3 Legacy 10L/10 Command Reference and Parameter Definitions).

To support the GNX Companion device:

1. Go to Devices > Serial.
2. Set the MG90's serial port for use as a LAN. This creates a LAN segment named "Serial LAN".

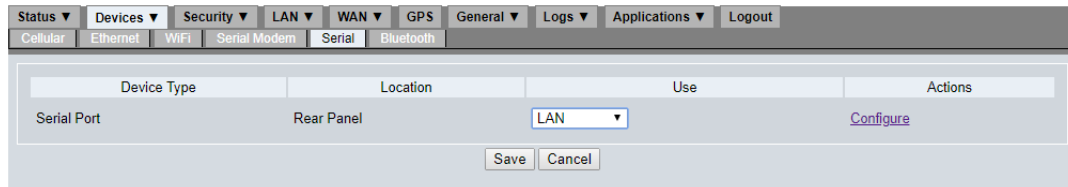


Figure 8-1: Configuring the serial port for GNX use

3. The serial port configuration defaults to the settings intended for the GNX companion device. Click Configure to adjust the serial port's Baud Rate and Flow Control, if necessary. See [Configuring the Serial LAN Segment](#) on page 68 for details.
4. Go to Applications > GNX.

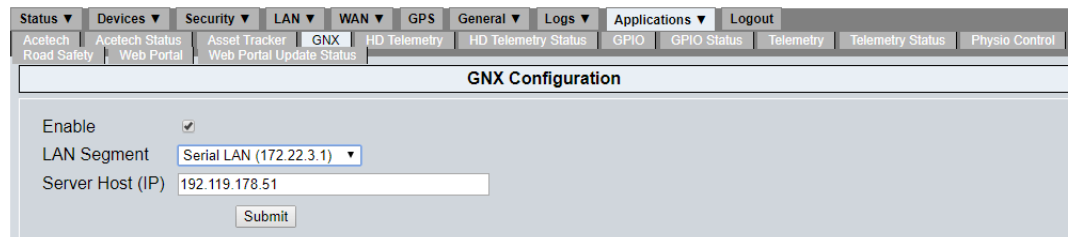


Figure 8-2: Configuring the GNX application

Device

5. Select Enable.
6. From the LAN Segment dropdown, select the Serial LAN.

Note: Do not select any of the other segments—the GNX device only supports connection over the Serial LAN.

7. In the Server Host (IP) field, enter the IP address of the GNX Config Server.
8. Click Submit.
9. Go to General > Shutdown.

The screenshot shows the 'Shutdown Configuration' page in the GNX AirLink Companion interface. The page has a top navigation bar with tabs: Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below this is a sub-navigation bar with tabs: Startup, Shutdown, Services, Tools, Backup/Restore, and Advanced Routing Rules. The 'Shutdown' tab is selected. The main content area is titled 'Shutdown Configuration' and contains the following settings:

High Voltage (volts)	36.0	(0.0v - 50.0v)
Low Voltage (volts)	11.0	(0.0v - 50.0v)
Low Voltage Alarm Hysteresis	0.9	(0.5v - 1.5v)
High Temperature (°C)	85.0	
Low Temperature (°C)	-30.0	
Uptime Extension After Ignition Off (hrs)	0.25	(0 - 25.5)
Button Reset Time (secs)	10	(0 sec - 255 sec)

At the bottom of the form are 'Save' and 'Cancel' buttons.

Figure 8-3: Configuring or adding a LAN segment

10. Set the Uptime Extension After Ignition Off to at least 0.25. (This keeps the MG90 on for 0.25 hours (15 minutes), which the GNX device requires to complete ongoing configuration modifications or firmware updates.)
11. Click Save.

9: Performance Tuning

The MG90 includes features that can be used to customize ('tune') its performance characteristics. These features includes:

- Load balancing—Optimize traffic carried over multiple WAN links. See [Configuring Load Balancing](#), below.
- Quality of Service—Define transmission performance requirements for traffic sent to the WAN and/or LAN. See [Setting Quality of Service \(QoS\)](#) on page 75.
- LAN throughput reporting—Track data usage via AMM. See [Configuring LAN Throughput Reporting Frequency](#) on page 76.

9.1 Configuring Load Balancing

The MG90 includes a load balancing feature that controls the amount of traffic carried over multiple active WAN links.

To use load balancing to take advantage of higher bandwidth links, lower cost links, etc., enable the feature on at least two WAN links:

1. Go to WAN > Links.
2. For each link to be used for load balancing:
 - a. Click Configure in the Actions column for the desired link.
 - b. Select Load Balanced.
 - c. Specify the Weight for the link. (See the Load balancing example below for details.)
 - d. Click Save.

Note: When traffic is being carried on load-balanced links, any links that are UP, not active, and not load-balanced will not carry any traffic.

Load balancing example

When load balancing is used, the MG90 uses each link's weight to calculate the load (percentage of total traffic) it will carry.

For example, if two links (LinkA and LinkB) are configured for load balancing:

Assume: LinkA_weight = 50; LinkB_weight = 100

LinkA_load = LinkA_weight / (LinkA_weight + LinkB_weight) = 50 / 150 = 33%

LinkB_load = LinkB_weight / (LinkA_weight + LinkB_weight) = 100 / 150 = 67%

Therefore: LinkB will be used to handle twice as much traffic as LinkA.

Note: Load balancing is accomplished by randomly assigning TCP sessions or UDP packet streams to connected WAN links participating in the load balanced group. Therefore, load balancing is NOT link bonding (i.e. datagrams from a single session sent over multiple WAN connections).

9.2 Setting Quality of Service (QoS)

The MG90 supports Quality of Service policies (networking rules) for router traffic, to ensure minimum or maximum performance for specific applications or services. QoS policies can be created for:

- The entire WAN or individual WAN links, including VPN traffic (since QoS policies are applied to traffic queued for the WAN link before the traffic is encrypted)
- The entire LAN or individual LAN segments

QoS policies can be applied to traffic between the MG90 and specified WAN or LAN entities. Depending on the connection type (WAN or LAN) and the source and destination addresses used, policies apply to incoming traffic (ingress), outgoing traffic (egress), or both directions.

Important: *If you create multiple QoS policies, ensure the settings in different policies don't conflict with each other.*

9.2.1 Defining QoS Policies

Defining WAN QoS policies

To define a WAN QoS policy:

1. Go to WAN > Networking Rules.
2. Select QoS Prioritizing in the drop-down and click Add New Networking Rule.
3. Enter a descriptive name in the Rule Name field.
4. Configure the fields. For detailed field information, see [WAN > Networking Rules](#) on page 220.
5. Click Save.

Defining WAN link QoS policies

To define a WAN Link QoS policy:

1. Go to WAN > Links.
2. Click Networking Rules in the Actions column for the link.
3. Select QoS Prioritizing in the drop-down and click Add New Networking Rule.
4. Enter a descriptive name in the Rule Name field.
5. Configure the fields. For detailed field information, see [WAN > Networking Rules](#) on page 220.
6. Click Save.

Defining LAN QoS policies

To define a LAN QoS policy:

1. Go to LAN > Networking Rules.
2. Select QoS Prioritizing in the drop-down and click Add New Networking Rule.
3. Enter a descriptive name in the Rule Name field.
4. Configure the fields. For detailed field information, see [WAN > Networking Rules](#) on page 220.
5. Click Save.

Defining LAN segment QoS policies

To define a LAN Segment QoS policy:

1. Go to LAN > LAN Segments.
2. Click Networking Rules in the Actions column for the segment.
3. Select QoS Prioritizing in the drop-down and click Add New Networking Rule.
4. Enter a descriptive name in the Rule Name field.
5. Configure the fields. For detailed field information, see [WAN > Networking Rules](#) on page 220.
6. Click Save.

9.3 Configuring LAN Throughput Reporting Frequency

If you have an AMM account through Sierra Wireless, or operate your own AMM server, the MG90 can automatically send LAN Throughput data (LAN traffic statistics) to AMM for data usage reporting and device management.

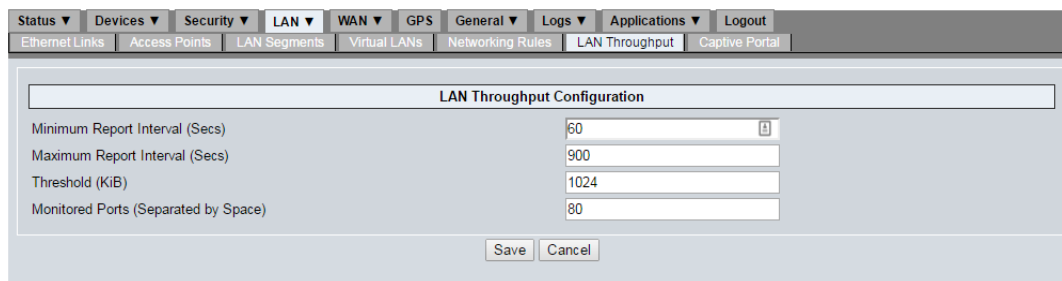
The reporting frequency is based on LAN Throughput Configuration options:

- Threshold — Automatically send a report when this much data has been collected, as long as the Minimum Report Interval has elapsed.
- Minimum Report Interval — Wait at least this long between sending reports. even if the Threshold amount of data has been collected.
- Maximum Report Interval — Wait no longer than this between sending reports. Automatically send a report even if the Threshold amount of data has not been collected.

Recommendation: Use the MG90's default interval and threshold values to maintain the optimum frequency for sending the LAN Throughput report.

To configure the reporting frequency:

1. Go to LAN > LAN Throughput.



LAN Throughput Configuration	
Minimum Report Interval (Secs)	60
Maximum Report Interval (Secs)	900
Threshold (KiB)	1024
Monitored Ports (Separated by Space)	80
Save Cancel	

Figure 9-1: LAN Throughput Configuration

2. Configure the fields. For detailed field information, see [LAN > LAN Throughput](#) on page 163.
3. Click Save.

10: How to configure a VPN

The MG90 can be configured to provide access to one or more Virtual Private Networks (VPNs). A VPN allows LAN devices connected to the MG90 to access an enterprise network and vice-versa.

The MG90 supports the following VPNs and VPN-related technologies:

- IPsec VPNs — LAN to LAN (most common) and Host to LAN.
See source.sierrawireless.com for documentation on configuring IPsec VPNs for the MG90.
- Certificates and pre-shared keys

Note: A management tunnel VPN is provided for communication between the MG90 and AMM. This VPN can be configured as required, but cannot be deleted.

10.1 Details Required to Configure VPNs

A VPN is configured on the MG90 by creating a VPN profile with settings that match those of a VPN server.

Before you can configure a VPN, you need the following information:

- MG90
 - LAN IP Subnetwork
 - LAN Mask
 - LAN IP Address
 - Security components such as pre-shared key, certificates etc.

Note: Using pre-shared keys (PSK) for authentication on some VPN servers will require the MG90 to have a static IP on the WAN interface used for VPN.

- VPN Server
 - Server IP Address
 - Destination Network IP Address
 - Destination Network Mask
 - Security components such as pre-shared key, server certificates etc.

10.2 Configuring VPN Profiles

To configure a new VPN Profile:

1. Ensure one or more WAN links have been properly configured as described in [Basic WAN Link Configuration](#) on page 39.
2. Ensure one or more LAN segments have been configured as described in [Configuring LAN Segments](#) on page 65.

3. Go to WAN > VPNs.

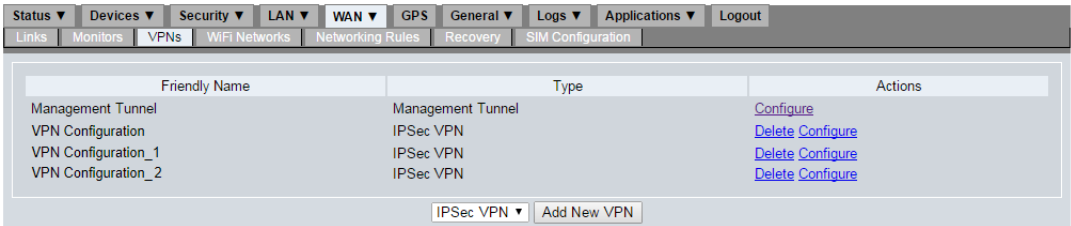


Figure 10-1: VPN Listing Screen

4. Click Add New VPN. (Note — The drop-down beside the button indicates IPsec VPN — This is the only option.)
5. Configure the VPN fields with the settings of the VPN server being used. For detailed field information, see [IPsec VPN Configuration \(WAN > VPNs > Add New VPN, and WAN > VPNs > \(IPsec VPN\) > Configure\)](#) on page 204.
- Note — If the VPN uses certificate authentication, the certificate’s key algorithm must be ECDSA if the MG90 is FIPS-enabled, or RSA if it is not FIPS-enabled.
6. Click Save.

Recommendation: When first testing a VPN, temporarily disable monitors to test that all other configuration parameters are working properly.

To update an existing VPN Profile:

1. Go to WAN > VPNs.

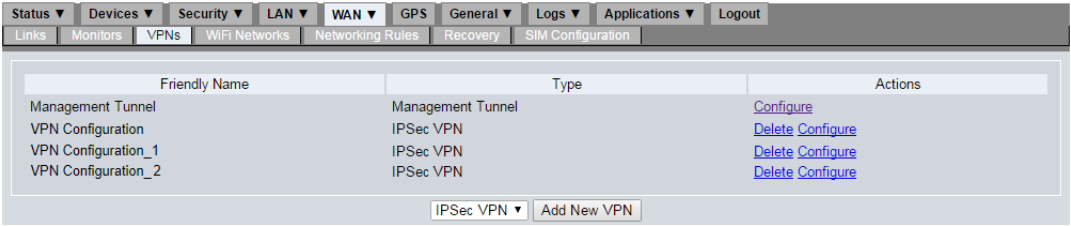


Figure 10-2: VPN Listing Screen

2. Click Configure in the Action column for the VPN profile to modify.
3. Configure the VPN fields with the settings of the VPN server being used. For detailed field information, see [IPsec VPN Configuration \(WAN > VPNs > Add New VPN, and WAN > VPNs > \(IPsec VPN\) > Configure\)](#) on page 204.
4. Click Save.
5. Reboot the MG90.

Important: The MG90 must be rebooted after making changes to an existing VPN profile for the changes to take effect.

Recommendation: When first testing a VPN, temporarily disable monitors to test that all other configuration parameters are working properly.

10.3 Setting Up Dead Peer Detection (DPD)

An MG90 VPN profile can be configured to send packets to a VPN server in an effort to detect dead connections. Doing so helps speed up reconnection to a VPN server.

To detect dead connections:

1. If the VPN uses:
 - IKEv1 — Enable Dead Peer Detection (DPD) on the VPN configuration screen to detect when a VPN service is down.
 - IKEv2 — If multiple WAN links are available, Sierra Wireless recommends:
 - Enable MOBIKE, which will automatically switch links when one goes down.
 and
 - Disable DPD because it can interfere with the fast switching provided by MOBIKE.
 MOBIKE has been tested by Sierra Wireless against Sierra Wireless' ACM VPN server. For more information on compatibility with VPN servers contact Sierra Wireless Technical Support for assistance (see [Contact Information](#) on page 3).
2. Sierra Wireless recommends that a monitor be configured to detect a dead connection to the VPN server and to attempt to reconnect to it. For information on creating a monitor, see [Using WAN Monitors to Detect Lost Connections](#) on page 49.
 - a. Create the monitor with the following settings:
 - Host — Set to a host that can be reached only through the VPN
 - Source Address — Set to a LAN segment assigned to the VPN.
 - b. In the VPN Configuration screen, assign the monitor to the VPN profile by selecting it in the Monitors field.

10.4 Multi-VPN Support

The multi-VPN feature allows each WAN link to have:

- 1 or more simultaneous LAN-to-LAN VPN tunnels (connections) by using the “Connect All” connection method, or
- 1 VPN tunnel at a time, with failover to alternate tunnels if the current tunnel cannot be established, by using the “Connect One” connection method.

Failover methods include:

- Random — Provides basic load-balancing across multiple VPN servers.
- Round Robin — Redundant failover to next available tunnel (static failover order from one VPN to the next, etc.). Next tunnel is selected based on alphabetical sorting of the VPNs' Friendly Name values. (e.g. If available VPNs are VPN#2 (“Remote Alt VPN”) and VPN#3 (“Local Alt VPN”), VPN#3 is used.)

The multi-VPN feature has the following attributes and restrictions:

- Each WAN link/Wi-Fi network can have up to 10 VPNs.
- If a WAN link/Wi-Fi network has multiple VPNs:
 - If “Connect All” connection method is used, all VPNs must be in LAN-to-LAN mode.
 - If “Connect One” connection method is used, all VPNs must be in HOST-to-LAN mode, or all must be in LAN-to-LAN mode.
 - All of the VPNs must use IKEv2. Do not use IKEv1 for any VPNs.

Warning: Creating a VPN profile using IKEv1 will affect the network hand-off performance of other VPN profiles using MOBIKE. This is true even when the IKEv1 profile is not selected in any WAN link.

- Each VPN tunnel can have distinct ping monitors.
- The LCI validates the address spaces to ensure there is no collision between VPNs applied to the same WAN link.
- The MG90 controls bandwidth to ensure a single VPN does not consume all available bandwidth on a WAN link.
- If the 'Connect All' connection method is in use, any two VPNs can have overlapping local subnets or overlapping remote subnets, but not both.

	Local Subnets		Remote Subnets	
Example 1	(VPN1) 172.22.1.0/24 (VPN2) 172.22.2.0/24	✓	(VPN1) 192.168.2.0/24 (VPN2) 192.168.1.0/24	<u>Valid configuration</u> Local subnets do not overlap. Remote subnets do not overlap.
Example 2	(VPN1) 172.22.1.0/24 (VPN2) 172.22.2.0/24	✓	(VPN1) 192.168.0.0/16 (VPN2) 192.168.1.0/24	<u>Valid configuration</u> Local subnets do not overlap. Only remote subnets overlap — VPN2 remote subnet is inside VPN1 remote subnet.
Example 3	(VPN1) 172.22.1.0/24 (VPN2) 172.22.1.0/24	✓	(VPN1) 192.168.2.0/24 (VPN2) 192.168.1.0/24	<u>Valid configuration</u> Only local subnets overlap. Remote subnets do not overlap.
Example 4	(VPN1) 172.22.1.0/24 (VPN2) 172.22.1.0/24	✗	(VPN1) 192.168.0.0/16 (VPN2) 192.168.1.0/24	<u>Not a valid configuration</u> Local subnets overlap. AND Remote subnets overlap — VPN2 remote subnet is inside VPN1 remote subnet.

Recommendation: To avoid conflicts with VPN profiles that are being used for WAN links, delete any VPN profiles that are not going to be used.

10.4.1 Configure WAN Links for Multi-VPN

Multi-VPN support is configured separately for each WAN link.

To configure multi-VPN support for a specific WAN link:

1. For:
 - Cellular WAN links — Go to WAN > Links > Configure.
 - Ethernet WAN links — Go to WAN > Links > Configure.
 - Wi-Fi networks — Go to WAN > WiFi Networks > Configure.
2. Select the desired VPN profiles in the VPN field:

The screenshot shows the 'Cellular WAN Link Configuration' page for a 'Sierra Wireless MC74XX @ MiniCard USB3 CA (Cellular A)' device. The page is divided into several sections with various settings:

- High Cost Link:** ☐
- MTU Size:** ☒ Automatic, ☐ Manual (with a text input field)
- Masquerade:** ☒
- Masquerade Port Range:** ☐ Automatic, ☒ Manual (with 'Minimum Port Number' set to 49152 and 'Maximum Port Number' set to 65535)
- Automatic DNS:** ☒
- Primary DNS:** (text input field)
- Secondary DNS Servers:** (text input field) comma-separated IP addresses
- Enable Private Zone:** ☐
- Number of Private Zone:** 1 (dropdown)
- APN:** sp.telus.com (text input field)
- Allow Blank APN:** ☐
- Signal Strength Filter Length:** 10 (text input field)
- Signal Strength Change Threshold (dBm):** 5 (text input field)
- Setting for Band:** All Bands (dropdown)
- Custom Band Setting Mode:** Exclude Bands (dropdown) with a text input field 4 comma-separated bands
- Use Management Tunnel:** ☒
- Pilot Ping:** ☐
- Monitors:** ☒ DefaultMonitor ☐ monitor 2
- Monitor Mode:** Success in one monitor keeps the link up (dropdown)
- VPN:**
 - ☐ VPN Configuration ☐ VPN Configuration_1 ☐ VPN Configuration_2
 - ☒ Connect One
 - ☒ Random
 - ☐ Round Robin - Alphanumeric Order
 - ☐ Connect All
- Load Balanced:** ☐

Figure 10-3: Selecting Multiple VPNs (Cellular Link example shown)

3. If more than one VPN profile was selected, select the connection method.
4. Click Save.

10.4.2 View Assigned VPNs

To view the VPNs that are assigned to a WAN link:

1. Go to Status > WAN.
2. Select Show Extended Status.

3. The VPN details appear in the link's IPsec VPN Info section:

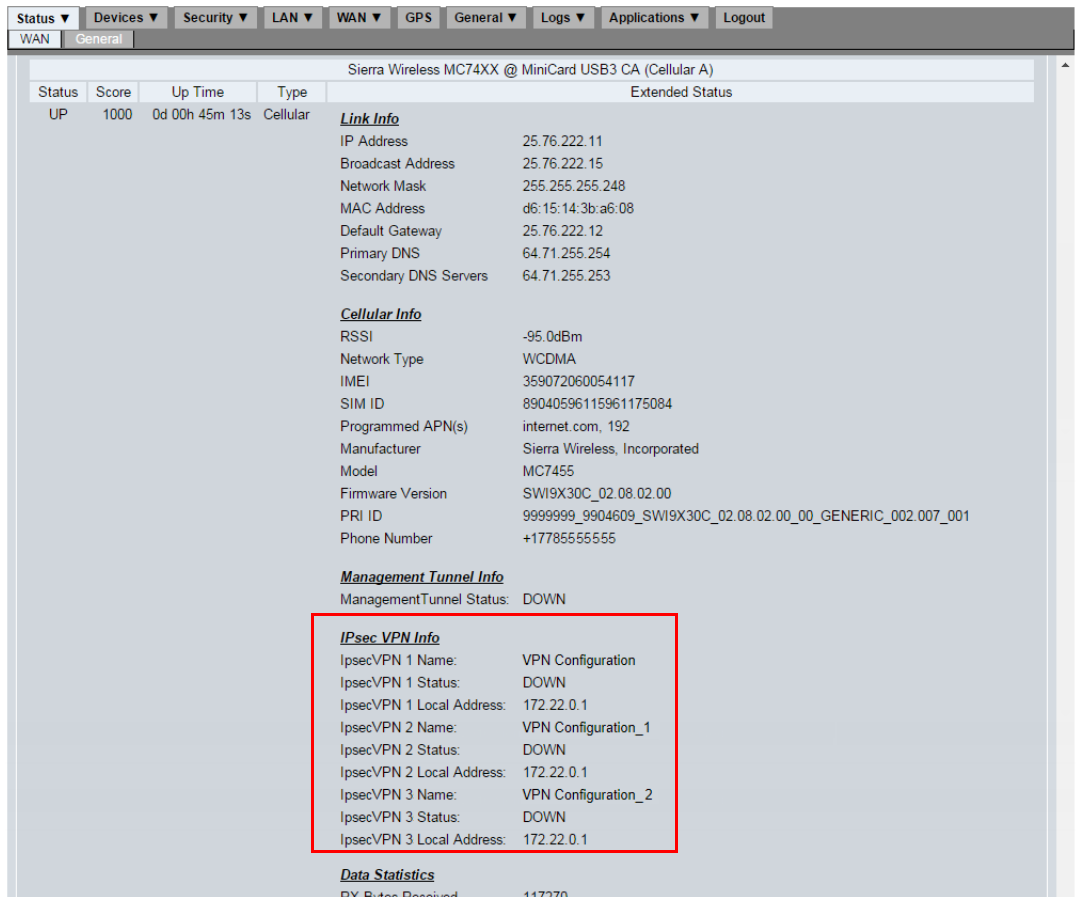


Figure 10-4: Viewing the VPNs assigned to a WAN Link

10.5 Configuring DNS Zones for Private DNS Server Use

In deployments that make use of VPNs with internal DNS servers (to resolve specific internal domains) and public DNS servers, the MG90 must be configured to use DNS zones.

Important: The preferred method for configuring private DNS zones (*LCI WAN Link Private Zone Configuration*) is via WAN interface configuration in the LCI for Ethernet, Cellular, and Wi-Fi networks. The legacy method (*Manual Private Zone Configuration*) should not be used to configure new private DNS zones.

Note: Private zones created in the Link Configuration screens are independent of the zones defined by the legacy method.

10.5.1 LCI WAN Link Private Zone Configuration

In the Ethernet or Cellular WAN Link Configuration screens, use the Private Zone fields to define up to 10 private zones.

The screenshot shows the 'Cellular WAN Link Configuration' window for a Sierra Wireless MC74XX @ MiniCard USB3 CA (Cellular A) device. The 'Enable Private Zone' checkbox is checked, and the 'Number of Private Zone' is set to 2. A table below shows two private zones configured with domain names and IP addresses. The table is highlighted with a red border.

Private Zone	Domain Name	Private Zone IP	Action
Private Zone 1	test1.com	11.11.11.11	Delete
Private Zone 2	test2.com	22.22.22.22	Delete

Figure 10-5: Private Zone Configuration

To configure up to ten private DNS zones for an Ethernet or Cellular WAN Link, or Wi-Fi Network:

1. In the LCI, go to WAN > Links or WAN > WiFi Networks and click Configure for the Ethernet link, Cellular link, or Wi-Fi network that will have private zones configured.
2. Select Enable Private Zone.
3. Select the Number of Private Zones to configure. A table of private zone fields will appear.
4. For each private zone being configured:
 - In Private Zone <#>, enter the domain name to be resolved by the internal DNS server.
 - In Private Zone IP <#>, enter the address of the internal DNS server.
5. Click Save.

To stop using private zones for a link or Wi-Fi network:

1. Deselect Enable Private Zone. The list of private zones is not deleted, and will re-appear if private zones are re-enabled.
2. Click Save.

To delete private zones:

1. Click Delete beside each zone to delete. The entry clears on-screen.
2. Click Save.

10.5.2 Manual Private Zone Configuration

The private zone configuration method described in this section is being replaced by the [LCI WAN Link Private Zone Configuration](#). Installations that have not used this method must use the LCI.

Note: Installations that have already used this method can continue to use it, as well as the preferred LCI method above.

To configure one or more MG90 routers for DNS zones:

1. In the LCI, set the Primary DNS and Secondary DNS Servers fields to the addresses of the public DNS servers to be used. (Applies to the WAN > Links configuration screens (Ethernet, Cellular) and WAN > Wi-Fi Networks configuration screen.)
2. Using a plain-text editor, create a DNS zones file named "private-zone.conf". In this file, indicate the domains to be resolved by the indicated internal DNS servers.

For example (filename: private-zone.conf):

```
zone "customer.local" IN {
    type forward;
    forward only
    forwarders { 10.5.1.1; 10.6.1.1; };
};
zone "customer.internal" IN {
    type forward;
    forward only;
    forwarders { 10.5.1.1; 10.6.1.1; };
};
```

In this example, the domains "customer.local" and "customer.internal" are both to be resolved by the internal DNS servers "10.5.1.1" or "10.6.1.1". Any other domains will be resolved by the public DNS servers specified in the WAN Link's Primary DNS and Secondary DNS Servers fields.

3. Use AMM to store the file on the MG90(s):
 - a. In AMM, select Config > Deploy F > Upload to copy the file to AMM.
 - b. Select Config > Deploy > Deploy to store the file on selected MG90 routers.

Note: Refer to [3] AirLink Mobility Manager Operation and Configuration Guide for details or contact Sierra Wireless Technical Support for assistance (see [Contact Information](#) on page 3).

11: Certificate Configuration

The MGOS certificate configuration process provides a simple, scalable method to obtain (enroll) and renew the signed certificates used for authentication in VPN and Wi-Fi networks.

- Certificate profiles are used to generate certificate signing requests (CSRs) and to hold the signed certificates after they are obtained. The private keys used for the CSR are automatically generated and stored on the device.
- Individual router certificate enrollment and renewal is supported in the LCI. (See [Certificate Profile Management](#), below.)
- Certificates are assigned in the LCI to VPNs and Wi-Fi networks that use certificate authentication by selecting from the available certificate profiles. (See [Using a Certificate Profile](#), below.)
- Fleet-wide certificate enrollment and renewal is managed via AMM. (For suggested procedures, refer to [4] Certificate Management via AMM, and for AMM details, refer to [3] AirLink Mobility Manager Operation and Configuration Guide.)
(Certificates can also be assigned via AMM configuration provisioning. Refer to [3] AirLink Mobility Manager Operation and Configuration Guide.)

Note: When upgrading from MGOS 4.2.x or earlier to MGOS 4.3 or later, existing certificates are automatically converted to certificate profiles.

Important: The enhanced certificate management process supports signed certificates containing **only** specific X.509 standard attributes (Distinguished Name and Subject Alternative Name). Customers are encouraged to use the new certificate creation method going forward ([LCI-initiated—Secure method](#) on page 86)—this method uses only the supported attributes.

Note also that certificates must be renewed (or replaced) by their expiry date. If a certificate expires, any VPNs and/or Wi-Fi networks using it will not connect.

11.1 Certificate Profile Management

Certificate profiles are created and maintained in Certificate Management (Security > Certificate Management). This feature is used to create and modify certificate profiles, each holding a CSR record that is used to obtain and store a signed certificate.

To use Certificate Management to configure CSRs and obtain and load signed certificates in certificate profiles:

1. Add a new profile and configure the certificate signing request attributes, or modify an existing profile if changes are needed to regenerate the CSR.
2. Generate and download the CSR.
3. Submit the CSR to a certificate signing authority (CSA) and receive a signed certificate and a CA certificate.

Important: Make sure the CSA is aware that the signed certificate must contain only the attributes from the CSR. If any other attributes are added to the certificate by the CSA, the certificate may not work. Even if the certificate with unsupported attributes can be uploaded and deployed, it cannot be used for generating a new CSR.

4. Upload the signed certificate to the router.
 5. Use the certificate on VPNs or Wi-Fi access points that use certificate authentication.
-

11.1.1 Certificate Enrollment Methods

MGOS supports LCI-initiated certificate enrollment for individual devices and AMM-initiated certificate enrollment for groups of devices.

11.1.1.1 LCI-initiated — Secure method

This is the recommended certificate enrollment method for a single device using the LCI, as illustrated in [Figure 11-1](#) (below). Using this method, the user generates a CSR file on the router, supplies it to a CSA and receives a signed certificate file and CA certificate, and uploads the certificate to the router.

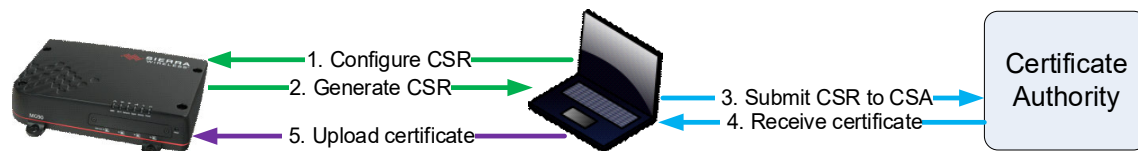


Figure 11-1: LCI-initiated Secure Method

To use this method to get and load a new certificate in a new certificate profile:

1. Go to Security > Certificate Management.
2. If you are:
 - Creating a new profile — In the dropdown list, select configure New CSR, and then click Add New Profile.

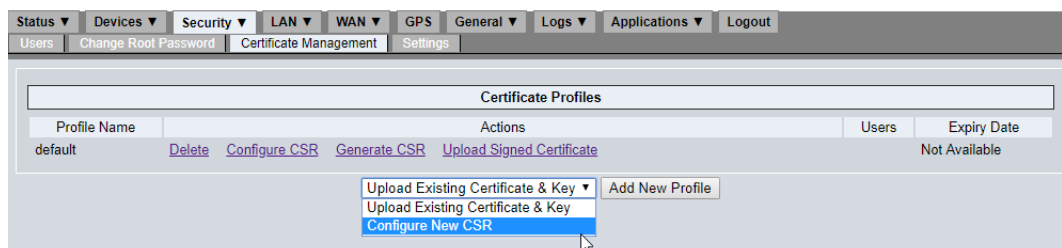


Figure 11-2: Option—Configure New CSR

- Modifying the attributes in a profile before getting a new certificate — Click Configure CSR for the profile being modified.

3. Enter/modify the CSR details:

Figure 11-3: CSR Configuration (New CSR or Modifying existing CSR)

- a. If this is a new CSR, enter a unique certificate Profile Name to identify it.
 - b. Select the appropriate Key Algorithm, Key Size, and Signature Algorithm to use for the requested certificate.
Important — If the requested certificate will be used for a VPN, the Key Algorithm must be ECDSA for a FIPS-enabled MG90, or RSA for a non-FIPS MG90.
 - c. Enter the Distinguished name fields. (The Common Name is required.)
 - d. If necessary, enter the Subject Alternative Name fields.
 - e. Click Save. The CSR details are stored in a certificate profile identified by the Friendly Name (Profile Name) you entered.
At this point, the CSR is configured, but a CSR file has not been created.
4. In the Certificate Profiles list, click Generate CSR for the configured profile.
 5. In the Certificate Signing Request Summary screen, click Generate CSR. A CSR file is stored in your browser's 'downloads' folder using the Profile Name.
 6. Submit the CSR file (downloaded from the device) to a CSA to obtain a signed certificate file and CA certificate.

Important: Make sure the CSA is aware that the signed certificate must contain only the attributes from the CSR. If any other attributes are added by the CSA, the certificate may not work. Even if the certificate with unsupported attributes can be uploaded and deployed, it cannot be used for generating a new CSR.

7. Once the signed certificate file is available, in the Certificate Profiles list, click Upload Signed Certificate for the configured profile.
8. In the Signed Certificate Upload screen, click Choose File and select the signed certificate file.
9. Click Save. The certificate's Expiry Date will appear in the Certificate Profiles list.

For detailed field information, see [Security > Certificate Management](#) on page 135.

11.1.1.2 LCI-initiated — Legacy method

This is the certificate enrollment method used in earlier MGOS releases for a single device using the LCI, as illustrated in [Figure 11-1](#) (below). Using this method, the user generates a CSR file and private key externally (outside the router), supplies them to a CSA and receives a signed certificate file and CA certificate, and uploads the certificate and private key file to the router.

Note: For security reasons and improved management features, the secure method described in section 11.1.1.1 (above) is recommended instead of this legacy method.

Important: A 'legacy' certificate converted when upgrading from MGOS 4.2.x or earlier will automatically be associated to the original usage (VPN or Wi-Fi network). However, if it has any unsupported attributes, the record may not render cleanly in the CSR Configuration screen and a CSR cannot be generated from those attributes. In this case, a new certificate profile is needed to generate a new CSR and obtain and load a new signed certificate to replace the existing certificate before it expires.

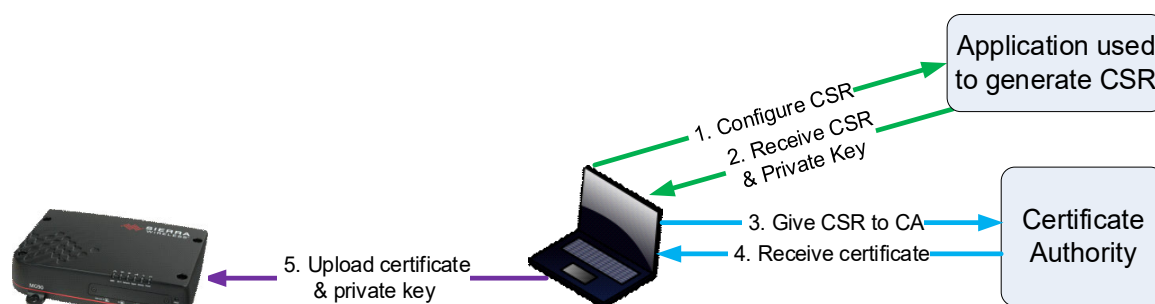


Figure 11-4: LCI-initiated Legacy Method

To use this method to get and load a new certificate in a new certificate profile:

1. Externally (outside the device), create and submit a CSR and a private key file to a CSA to obtain a signed certificate file and CA certificate.

Important: Make sure the CSA is aware that the signed certificate must contain only the X.509 standard attributes listed below. (If any other attributes are added by the CSA, the certificate may not work. Even if the certificate with unsupported attributes can be uploaded and deployed, it cannot be used for generating a new CSR.)

Supported X.509 standard attributes:

- Distinguished Name (Common name, Department name, Organization name, City, State/Province, Country Code)
- Subject Alternative Name (Email address, Domain name, IP address, URI, User principal name)

2. Go to Security > Certificate Management.
3. In the dropdown list, select Upload Existing Certificate & Key.
4. Click Add New Profile. The Existing Certificate/Key Upload screen appears.
5. Enter a unique certificate Profile Name.
6. Select the Certificate File Type (PEM or PFX).
7. Click the first Choose File button to select the signed certificate file.
8. (PFX certificate only) Enter the PFX password in the PFX Import Password field.

9. (PEM certificate only) Click the second Choose File button to select the Private Key file that was used to create the certificate.
10. Enter the private key file's password in the Private Key Password field. (This is required for both certificate types—the private key file is embedded in the PFX certificate.)
11. Click Save. The certificate's Expiry Date will appear in the Certificate Profiles list.

For detailed field information, see [Security > Certificate Management](#) on page 135.

11.1.1.3 AMM-initiated—Secure method

This method allows AMM to initiate and drive the certificate enrollment process for multiple devices. For details, refer to [3] AirLink Mobility Manager Operation and Configuration Guide.

11.1.2 Renewing a Certificate

To renew an expiring certificate, use the procedure below.

Important: *Certificates can only be renewed if their CSRs contain valid X.509 attributes. If a certificate was created and loaded using the legacy method and has unsupported attributes, its details will not render cleanly in the CSR screen and the certificate cannot be renewed. In this case, create and load a new certificate in a new profile ([LCI-initiated—Secure method](#) on page 86), then use the new profile in affected VPNs and Wi-Fi networks.*

1. Go to Security > Certificate Management.
2. Make any required changes to the profile—click Configure CSR in the Certificate Profiles list, make the changes, and click Save.

Figure 11-5: CSR Configuration

3. Generate the CSR file—click the Generate CSR link in the Certificate Profiles list, and then click the Generate CSR button to save the CSR file in your browser's "downloads" folder using the Profile Name.

4. Submit the CSR file (downloaded from the device) to a CSA to obtain a signed certificate file and CA certificate.

Important: Make sure the CSA is aware that the signed certificate must contain only the attributes from the CSR. If any unsupported attributes are added by the CSA, the certificate may not work and this profile cannot be used to regenerate the CSR.

5. Once the signed certificate file is available, in the Certificate Profiles list, click Upload Signed Certificate for the configured profile.
6. In the Signed Certificate Upload screen, click Choose File and select the signed certificate file.
7. Click Save. The certificate's Expiry Date will appear in the Certificate Profiles list.

The new certificate will now be used by the VPNs and Wi-Fi networks that were configured to use this profile.

11.1.3 Deleting a Certificate Profile

To delete an existing certificate profile:

1. Go to Security > Certificate Management.
2. In the Certificate Profiles list, click Delete for the profile you want to remove.
3. When prompted, click OK to confirm the profile deletion.

Note: Any VPNs or Wi-Fi networks that were configured to use the deleted profile must be updated to use a different profile in order to connect.

11.2 Using a Certificate Profile

Certificate profiles are used when configuring:

- VPN profiles — In the IPsec VPN Configuration screen (WAN VPNs > Configure), a certificate profile must be selected if the Authenticate Method is "Certificate".
- Wi-Fi networks — In the WiFi Network Configuration screen (WAN > WiFi Networks > Configure), a certificate profile must be selected if the Authentication setting is "EAP-PEAP" or "EAP-TLS".

Note: The certificate profiles shown in the examples below are configured in the Certificate Management screen (Security > Certificate Management). See [Certificate Configuration](#) on page 85 for details.

Status▼Devices▼Security▼LAN▼WAN▼GPS▼General▼Logs▼Applications▼Logout

LinksMonitorsVPNsWiFi NetworksNetworking RulesRecoverySIM Configuration

IPsec VPN Configuration

Friendly Name

ACM_IPsec_Cert longname

Server Address

208.81.123.123

Server ID

C = CA, ST = BC, O = Sierra

Remote Network

Remote Subnets

192.168.1.0/24

Comma separated CIDR notation

Allow Management Tunnel Bypass

☒

IPsec Address Exemptions

Comma separated IP or hostname.

Local Termination

Network▼

Local Subnets

☐ Default LAN - 172.22.0.0/24

☒ Serial LAN - 172.22.1.0/24

Gateway Virtual IP

☒ Automatic(IKEv2 Only)

☐ Manual

Internet Key Exchange

IKEv2▼

IKE Transform

aes256-sha2_256 dh-group 14▼

MOBIKE

☒

Dead Peer Detection

☒

Delay (sec)

10

Timeout (sec)

30

IKE Lifetime (min)

60

Reauthenticate on IKE ReKey

☒

IPsec

ESP Transform

aes256-sha2_256 dh-group 14▼

IP Compression

☐

Force UDP Encapsulation

☒

Authentication

Authentication Method

Certificate▼

Auth ID

ESN▼ND60510040011018

CA Certificate File

Choose File

No file chosen

(installed)

Certificate Profile

☒ J-Cert

☐ W-Cert

☐ default-Cert

Figure 11-6: VPN—Certificate Profiles

Figure 11-7: WiFi Networks — Certificate Profiles

To use a certificate file with a VPN or Wi-Fi network:

1. Select the Certificate Profile that contains the certificate to be used.
2. Upload the corresponding CA certificate file — click Choose File and load the file from your computer.

Note: Only one CA file can be uploaded. If the CSA provided separate root and intermediate CA certificates, create a combined file — see [Creating a combined CA certificate](#), below.

11.2.1 Creating a combined CA certificate

If the CSA (Certificate Signing Authority) provides separate root and (1 or more) intermediate CA certificates, these must be merged into a single combined CA certificate file before loading into a VPN configuration.

To merge root and intermediate CA certificates:

1. If there are multiple intermediate certificates, arrange them according to the chain list provided by the CSA.
2. Open a new file in a plain-text editor (e.g. Notepad, gedit, etc.).
3. Paste the root certificate, followed by the intermediate certificate(s) into the file in the required order (from [step 1](#)).
4. Save the file.

The combined file can now be loaded into the appropriate VPN configuration.

If the file does not work for a given VPN server, confirm the required CA file format (e.g. root followed by intermediate certificates, or intermediate certificates followed by root) with the server provider, and rebuild the file if necessary.

12: Setting up GPS connectivity

The MG90 provides GPS connectivity via the following devices types:

- Internal GPS receiver — Pre-equipped. This is the default GPS device.
- External GPS device— Optional device connected via a serial or USB connection, or through Ethernet (using the UDP protocol).

The GPS location data can be:

- Reported to an AMM and the customer's mapping system.
- Forwarded over the WAN to additional servers with a static IP address or host name.
- Forwarded over the LAN to a local host.
- Forwarded to a device connected to the MG90's serial port.

Note: If the MG90's internal GPS is used, any TAIP or NMEA message can be forwarded locally or remotely.

If an external GPS source is used, any TAIP message or NMEA RMC message can be forwarded locally or remotely. (No other NMEA message types can be forwarded.)

The MG90 also supports Dead Reckoning, which is a feature that uses the MG90's built-in inertial sensors to provide location reporting. Dead Reckoning operates alongside satellite (GNSS) navigation, and maintains location tracking capability when a GNSS signal is impaired or temporarily unavailable.

The MG90 uses its last known GNSS position along with sensor input to calculate vehicle position. For example, when the vehicle enters a tunnel, parking garage, or urban canyon, Dead Reckoning data augments data from the weakened GNSS signal and helps maintain accurate location reporting.

Dead Reckoning can operate just using the MG90's integrated sensors, or with speed input (if available) from an OBD-II or HDOBD connection.

12.1 GPS Configuration Set Up

Status ▾	Devices ▾	Security ▾	LAN ▾	WAN ▾	GPS ▾	General ▾	Logs ▾	Applications ▾	Logout												
GPS Configuration																					
Expand All																					
Enable ☒																					
GPS Sources																					
<table border="1"> <tr> <td> Built-in GPS ☒ Enable Jitter Filter ☐ Enable DR ☐ Clear Calibration Data </td> <td> External GPS via UDP Port ☐ Source Name: ExtUDP UDP Port: 5068 </td> <td> External GPS via Serial or USB ☐ Source Name: ExtSerial Device Attachment: ☐ Rear Panel Serial ☐ USB Port </td> </tr> </table>										Built-in GPS ☒ Enable Jitter Filter ☐ Enable DR ☐ Clear Calibration Data	External GPS via UDP Port ☐ Source Name: ExtUDP UDP Port: 5068	External GPS via Serial or USB ☐ Source Name: ExtSerial Device Attachment: ☐ Rear Panel Serial ☐ USB Port									
Built-in GPS ☒ Enable Jitter Filter ☐ Enable DR ☐ Clear Calibration Data	External GPS via UDP Port ☐ Source Name: ExtUDP UDP Port: 5068	External GPS via Serial or USB ☐ Source Name: ExtSerial Device Attachment: ☐ Rear Panel Serial ☐ USB Port																			
NMEA Messaging																					
<table border="1"> <tr> <th>Local</th> <th>Remote</th> </tr> <tr> <td>Sentences: GSV,GGA,RMC</td> <td>Sentences:</td> </tr> <tr> <td>Report Interval: 5</td> <td>Report Interval: 10</td> </tr> <tr> <td colspan="2"> Additional Options Emit ESN in Proprietary Sentence ☐ Group Sentences in a Single UDP Packet ☐ </td> </tr> </table>										Local	Remote	Sentences: GSV,GGA,RMC	Sentences:	Report Interval: 5	Report Interval: 10	Additional Options Emit ESN in Proprietary Sentence ☐ Group Sentences in a Single UDP Packet ☐					
Local	Remote																				
Sentences: GSV,GGA,RMC	Sentences:																				
Report Interval: 5	Report Interval: 10																				
Additional Options Emit ESN in Proprietary Sentence ☐ Group Sentences in a Single UDP Packet ☐																					
TAIP Messaging																					
<table border="1"> <tr> <th>Local</th> <th>Remote</th> </tr> <tr> <td>Responses:</td> <td>Responses:</td> </tr> <tr> <td>Report Interval: 30</td> <td>Report Interval: 30</td> </tr> <tr> <td colspan="2"> Additional Options Enable ☐ Top of Hour: 0 Checksum ☒ CR/LF ☒ Vehicle ID: ~ </td> </tr> </table>										Local	Remote	Responses:	Responses:	Report Interval: 30	Report Interval: 30	Additional Options Enable ☐ Top of Hour: 0 Checksum ☒ CR/LF ☒ Vehicle ID: ~					
Local	Remote																				
Responses:	Responses:																				
Report Interval: 30	Report Interval: 30																				
Additional Options Enable ☐ Top of Hour: 0 Checksum ☒ CR/LF ☒ Vehicle ID: ~																					
Local Forwarding																					
<table border="1"> <tr> <th>TCP</th> <th>UDP</th> <th>Serial</th> </tr> <tr> <td>Listen Port: 9345</td> <td> Broadcast LAN ☒ Port: 5067 </td> <td> RS-232 ☐ Speed: B9600 DataBits: CS8 Parity: none StopBitX2 ☐ HW Flow ☐ </td> </tr> </table>										TCP	UDP	Serial	Listen Port: 9345	Broadcast LAN ☒ Port: 5067	RS-232 ☐ Speed: B9600 DataBits: CS8 Parity: none StopBitX2 ☐ HW Flow ☐						
TCP	UDP	Serial																			
Listen Port: 9345	Broadcast LAN ☒ Port: 5067	RS-232 ☐ Speed: B9600 DataBits: CS8 Parity: none StopBitX2 ☐ HW Flow ☐																			
Remote Forwarding																					
Remote client entries separated by spaces with format: <ip or hostname> <port> or <ip or hostname> <port>#<report interval [1,3600]>																					
Server List:																					
Forwarding Thresholds																					
Enable ☐ <table border="1"> <tr> <th>Time</th> <th>Speed</th> <th>Distance</th> </tr> <tr> <td>Slow Report Interval (secs): 30</td> <td>Speed Unit: ☐ mph ☒ km/h</td> <td>Distance Unit: ☐ yard ☒ meter</td> </tr> <tr> <td>Fast Report Interval (secs): 5</td> <td>Speed Change Threshold: 10</td> <td>Distance Change Threshold: 100</td> </tr> </table>										Time	Speed	Distance	Slow Report Interval (secs): 30	Speed Unit: ☐ mph ☒ km/h	Distance Unit: ☐ yard ☒ meter	Fast Report Interval (secs): 5	Speed Change Threshold: 10	Distance Change Threshold: 100			
Time	Speed	Distance																			
Slow Report Interval (secs): 30	Speed Unit: ☐ mph ☒ km/h	Distance Unit: ☐ yard ☒ meter																			
Fast Report Interval (secs): 5	Speed Change Threshold: 10	Distance Change Threshold: 100																			
Event Thresholds																					
<table border="1"> <tr> <th>Time</th> <th>Speed</th> <th>Distance</th> </tr> <tr> <td>Fastest Report Interval (secs): 5</td> <td>Speed Unit: ☐ mph ☒ km/h</td> <td>Distance Unit: ☐ yard ☒ meter</td> </tr> <tr> <td></td> <td>Critical Speed Threshold: 16</td> <td>Critical Distance Threshold: 100</td> </tr> <tr> <td></td> <td>High Speed Threshold: 3</td> <td>High Distance Threshold: 20</td> </tr> </table>										Time	Speed	Distance	Fastest Report Interval (secs): 5	Speed Unit: ☐ mph ☒ km/h	Distance Unit: ☐ yard ☒ meter		Critical Speed Threshold: 16	Critical Distance Threshold: 100		High Speed Threshold: 3	High Distance Threshold: 20
Time	Speed	Distance																			
Fastest Report Interval (secs): 5	Speed Unit: ☐ mph ☒ km/h	Distance Unit: ☐ yard ☒ meter																			
	Critical Speed Threshold: 16	Critical Distance Threshold: 100																			
	High Speed Threshold: 3	High Distance Threshold: 20																			
<table border="1"> <tr> <td>Accuracy Unit: ☐ yard ☒ meter</td> <td>Critical SBAS Status Event Reporting: ☒</td> </tr> <tr> <td>Critical Accuracy Threshold: 5</td> <td>Critical SBAS Interval (secs): 30</td> </tr> <tr> <td>Critical Accuracy Interval (secs): 30</td> <td></td> </tr> </table>										Accuracy Unit: ☐ yard ☒ meter	Critical SBAS Status Event Reporting: ☒	Critical Accuracy Threshold: 5	Critical SBAS Interval (secs): 30	Critical Accuracy Interval (secs): 30							
Accuracy Unit: ☐ yard ☒ meter	Critical SBAS Status Event Reporting: ☒																				
Critical Accuracy Threshold: 5	Critical SBAS Interval (secs): 30																				
Critical Accuracy Interval (secs): 30																					
Turn Based Forwarding & Reporting																					
Enable ☐ <table border="1"> <tr> <th>Time</th> <th>Rotation Speed</th> </tr> <tr> <td>Turn Report Interval (secs): 1</td> <td>Rotation Threshold (degrees/sec): 4.0</td> </tr> </table>										Time	Rotation Speed	Turn Report Interval (secs): 1	Rotation Threshold (degrees/sec): 4.0								
Time	Rotation Speed																				
Turn Report Interval (secs): 1	Rotation Threshold (degrees/sec): 4.0																				
Submit																					

Figure 12-1: GPS Configuration Screen—Expanded View

For detailed field information, see [Table F-1, GPS screen fields](#), on page 231.

To configure the GPS settings:

1. Go to the GPS tab.
2. Select Enable.

Note: The screen appears in 'collapsed' view. To expand or collapse any section (to view or hide its fields), click anywhere on the section's heading bar.

3. In the GPS Sources section, select the GPS source:
 - Built-in GPS
 - External GPS via UDP port (through WAN)
 - External GPS via Serial or USB
4. Optionally, if Built-in GPS is selected, Dead Reckoning can be enabled. To use the Dead Reckoning feature, follow [Configuring Dead Reckoning](#) on page 97.
5. If preferred, select Enable Jitter Filter to ignore small movements — this is useful for handling GPS error while the router is stationary.

Note: This may not be suitable if high-sensitivity reporting is required for very slow moving vehicles (slower than 1.5 km/h).

6. Configure the NMEA Messaging and TAIP Messaging if required.
If using TAIP Messaging, ensure the Enable checkbox under Additional Options is selected.
7. Configure the Local Forwarding options as required:
 - TCP/UDP — Allows data to be sent to the LAN using the respective protocol.
 - Serial — Allows data to be sent to a device connected to the MG90's serial port. (The MG90's serial port settings must match those of the receiving system.)
Note that Serial forwarding requires that the Serial port "Use" value be set to Application in the Devices > Serial tab.
8. Configure the Remote Forwarding options if required — Enter a space-separated list of IP addresses or host names to send the GPS data to.
9. Configure the Forwarding Thresholds options if NMEA/TAIP messages should be forwarded at variable intervals dependent on vehicle speed, distance traveled, and time elapsed.
 - To use variable interval reporting:
 - Select Enable. (The Report Interval fields in NMEA Messaging and TAIP Messaging will turn gray and not be considered.)
 - Set the maximum (Slow Report Interval) and minimum (Fast Report Interval) times between reports, regardless of speed and distance thresholds.
 - Set the speed threshold (change in speed since last report) that causes report to be forwarded.

For example:

 - If Fast Report Interval is 5 and the last report was sent ≥ 5 seconds ago, and
 - If Speed Change Threshold is 10.50 mph and the speed at the last report was 40.0 mph,
 - Then a report is immediately forwarded if the vehicle's speed drops to 29.50 mph or rises to 50.50 mph.
 - Set the distance threshold (change in position since last report) that causes report to be forwarded.

For example:

 - If Fast Report Interval is 5 and the last report was sent ≥ 5 seconds ago, and
 - If Distance Change Threshold is 100.25 meters,

- Then a report is immediately forwarded if the vehicle's location changes (since the last report) in any direction by 100.25 meters.
 - To use fixed interval reporting, deselect Enable, and use the Report Interval values in the TAIP Messaging Local and Remote sections.
10. Configure the Event Thresholds, which control how frequently GPS information will be broadcast to AMM.
 11. Configure the Turn Based Forwarding & Reporting options to report GNSS information when the vehicle is turning, since the MG90 may not meet the Speed and Distance forwarding thresholds during turns. (For details, see [Configuring Turn-based Forwarding and Reporting](#) on page 98.)

Important: *Turn detection requires the MG90 to be installed horizontally in the vehicle.*

- a. Select Enable.
 - b. Set the Turn Report Interval (time between reports) in seconds.
 - c. Set the Rotation Threshold in degrees per second. A report will be sent whenever the rotation speed is at least this value.
12. Click Submit.

12.2 Configuring Dead Reckoning

To configure the MG90 to use Dead Reckoning (DR):

1. In the GPS Configuration screen, select Enable DR.
2. Click Submit.
The Clear Calibration Data button becomes available.
3. Move the vehicle into an area with open sky to get a clear GPS fix.
4. Click Clear Calibration Data to clear old calibration information (if previously calibrated) and begin recalibrating.

Note: When Dead Reckoning is enabled, the initial calibration process begins automatically as soon as the vehicle is in motion with a GNSS antenna attached.

5. The calibration process can take anywhere from 5 to 30 minutes once the vehicle is in motion, depending on driving conditions. The Status > General screen will show the GPS DR Calibration Status as "In progress" once the calibration begins.

To shorten the calibration time, 'exercise' the sensors by performing multiple stops, starts, turns, and acceleration/deceleration on straight stretches.

For optimal calibration:

- Drive the vehicle in open sky conditions
- Undergo several turns
- Stop and start the vehicle several times in a straight line (braking for, and accelerating away from stop signs, for example)

6. When calibration is finished, the GPS DR Calibration Status on the Status > General page changes to “Complete”, and the MG90’s GNSS LED will reflect the current DR state.

Table 12-1: GNSS LED DR State Indication

Color	State
Solid Green	Satellite fix is available, and Dead Reckoning is inactive (disabled, or not calibrated)
Solid Blue	Satellite fix available, and Dead Reckoning is active
Flashing Blue	No satellite fix is available, and Dead Reckoning is active
Flashing Amber	No satellite fix is available, and Dead Reckoning is inactive (disabled, or not calibrated)
Off	GNSS is off or antenna is not attached.

12.3 Configuring Turn-based Forwarding and Reporting

MGOS also includes Turn-based Forwarding and Reporting options that allow more frequent reports to be made during turns, which will provide the application (AMM or another customer-provided application) receiving the data with a more complete path of travel during the turn.

Although Speed and Distance Forwarding Thresholds may be configured, vehicle speed typically decreases while turning such that these thresholds are not met. To ensure reports are sent while turning, Turn-based Forwarding and Reporting options can be enabled.

Important: *Turn detection requires the router to be installed horizontally in the vehicle.*

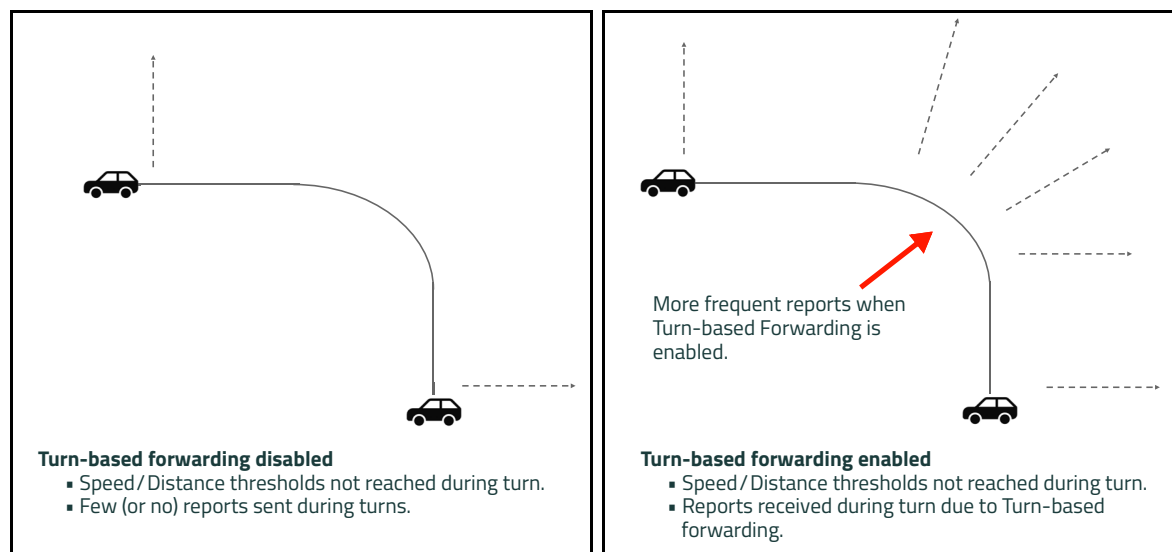


Figure 12-2: Effect of Turn-based Forwarding

To configure turn-based forwarding and reporting:

1. In the GPS Configuration screen’s Turn Based Forwarding & Reporting section, select Enable.
2. Set the Turn Report Interval to indicate how frequently reports must be sent. Use lower values to report more frequently.

3. Set the Rotation Threshold (the rotation speed) to send reports when the vehicle is turning at the specified speed (number of degrees per second). Use lower values to report more frequently.
4. Click Submit.

For detailed field information, see [Table F-1, GPS screen fields](#), on page 231.

13: Applications

Several value added applications are available for the MG90 that enhance and extend the MG90's capabilities.

See [Applications Tab](#) on page 254.

14: Updating the System

The router requires periodic updates of its operating software (MGOS) and the firmware running on its cellular radio modules.

These updates can be applied to the router and its modules as described below:

MGOS software updates

Software updates can be installed in the following ways:

- Over the air (OTA):
 - Initiated automatically by router — See [Configuring Auto Software Updates](#) on page 101 for details.
 - Initiated by AMM — AMM can send a notice to the router that forces it to download a specific software update from AMM. Refer to AMM documentation for details.
 - Initiated by user — See [Forcing an OTA Update](#) on page 104 for details.
- Manual USB flash drive installation — MGOS upgrade image can be downloaded from source.sierrawireless.com to a USB flash drive and installed manually. See source.sierrawireless.com/resources/airlink/software_downloads/airlink-mg-usb-images/ for details.
- Based on firmware settings, radio module firmware images may be downloaded along with MGOS software updates.

Radio module firmware updates

Radio module firmware images are stored in the router and installed/updated on the radio module(s) in the following ways:

- Automatically, initiated by the router — If a radio module image must be updated or switched (based on configuration settings), the router will download images from the AMM into internal storage if necessary when it boots, and install them on the modules.
- Automatically, initiated by changing a SIM — If enabled, the router will download the required image for the new SIM's carrier from the AMM into internal storage if necessary when it boots, and install it on the module.
- Initiated manually by user — The user can choose which images to load into internal storage, and can force specific images to be installed on the modules.

See sections [14.4.2](#)–[14.4.4](#) for details.

14.1 Configuring Auto Software Updates

The MG90 can be configured to check for and download updates OTA over a WAN link, including:

- Software updates for the MG90 — See [Downloading and Installing Auto Software Updates](#) on page 103.
- Firmware updates for cellular radio modules — See [Radio Module Firmware Images](#) on page 104.

To configure automatic software update download and installation:

1. Go to General > Auto Software Updates.

ND605100400110

Status ▾Devices ▾Security ▾LAN ▾WAN ▾GPS ▾General ▾Logs ▾Applications ▾Logout

StartupShutdownServicesToolsBackup/RestoreAdvanced Routing RulesAuto Software Updates

Automatic Software Update Configuration

Options

Enabled:☒

Allow Downgrade:☐

Upgrade Options:

☐ Download Updates Only

☒ Download and Apply Updates on Next Boot

☐ Download and Apply Updates during Scheduled Time (UTC time without DST)

Disable Boot Checks on Ignition Shutdown:☐

Download Bandwidth Limit (KB/s):

Download Timeout (Seconds):

Download on High Cost Link:☐

Radio Module Firmware Options

Firmware Upgrade Option:

Upgrade Active ▾

Firmware Upgrade on High Cost Link:☐

SIM-based Switching Enabled on CA:☒

SIM-based Switching Enabled on CB:☒

Radio Module Firmware Available

Active	Status	Module	Carrier	Firmware Version	Size (MB)	Upgrade Disabled	Force Firmware	Purge
CA	Available	MC7354	GENERIC	SWI9X15C_05.05.58.00_Generic_005.025_002	35	☐	None ▾	Never ▾
CB	Available	MC7455	GENERIC	SWI9X30C_02.30.03.00_GENERIC_002.046_001	65	☐	None ▾	Never ▾

Add Firmware

Remaining Disk Space (MB): 190

EM7511 ATT ▾Add

To Upload... Choose and Upload a File From Your Computer

Radio Module Current Status

Cellular CA

RM: MC7455

SIM: GENERIC

SIM ICCID: 89332404677726677726

SIM IMSI: 222094589795795

Firmware: 02.30.03.00_GENERIC_002.046_001

SKU PRI: 9904514

Carrier PRI: 9999999_9904609_SWI9X30C_02.30.03.00_00_GENERIC_002.046_001

SubmitCancel

Figure 14-1: Automatic Software Updates Configuration Options (Expanded View)

Note: The screen initially appears in a partially 'collapsed' view. To expand or collapse any section (to view or hide its fields), click anywhere on the section's heading bar.

2. In the Options section:
- a. Select Enabled to enable automatic updates, or deselect to disable.

b. Configure the remaining fields (see [Table G-8](#) on page 248 for detailed information):
 - Set the appropriate Upgrade Options to schedule update installations. See [Downloading and Installing Auto Software Updates](#) on page 103 for details.
 - Set the remaining Options to control download behavior.

Important: By default, Download on High Cost Link is not selected, so software downloads occur on low cost links only. If you select this option, firmware downloads can also occur over high cost links.

3. Click Submit.

14.2 Downloading and Installing Auto Software Updates

Downloading Auto Software Updates

If Auto Software Updates are:

- Enabled:
 - The MG90 automatically checks AMM for available software updates and downloads them:
 - After the MG90 has finished booting and the router is operational
 - When Automatic Software Update Configuration settings (General > Auto Software Updates tab) are changed (unless the change is to disable Auto Software Updates)
 - On a link switch
 - Software updates can also be manually downloaded OTA using the download-new-software-updates tool (see [Forcing an OTA Update](#) on page 104 for details).
- Disabled — Updates cannot be downloaded automatically via AMM, or manually via the download-new-software-updates tool). To load a software update, use the manual USB flash drive installation method described in [MGOS software updates](#) on page 101.

Installing Auto Software Updates

After updates have been downloaded to the MG90, they are installed based on the selected Upgrade Options:

- Download Updates Only — Updates are not automatically installed. To install any stored updates, select one of the other Upgrade Options. The updates will be installed as described for those options.
- Download and Apply Updates on Next Boot — (Default option) Updates install automatically when the MG90 boots.

Important: *If Disable Boot Checks on Ignition Shutdown is selected and the MG90 reboots because the ignition was turned off and then power was reapplied, the MG90 will not automatically check for available software updates.*

- Download and Apply Updates during Scheduled Time — Updates install automatically during a scheduled time slot ('Between'), based on the selected Attempt Upgrade option:
 - Just Once — Installation attempt occurs only during the scheduled date and time slot ('Between').
 - Every Day — Installation attempts can occur every day, beginning on the Start From date.
 - Every Week — Installation attempts can occur once per week, beginning on the Start From date.
 - Every Month — Installation attempts can occur once per month, beginning on the Start From date. If the Start From date is the last day of the month (e.g. 30 June), then attempts occur on the last day of each month (e.g. 31 January, 28 February, 31 March, 30 April, etc.)

Important: *For MG90 routers that contain two different Sierra Wireless cellular radio modules (e.g. MC7354 + MC7455, MC7455 + EM7511, etc.), make sure a SIM card is installed for at least one of the modules prior to an OTA firmware update. Otherwise, if firmware is downloaded OTA, the MG90 will not install the downloaded firmware, and will continue running its current version. In this case, to complete the upgrade:*

- *Install new firmware using a USB stick,*
 - or*
 - *Insert a SIM for one or both modules, select and run General > Tools > "clean-local-software-update-cache", and then reboot.*
-

Note: In cases where the MG90 is never shut off (i.e. when a vehicle is in operation 24 hours per day, 7 days per week), use the 'Scheduled Time' upgrade option to install updates.

While an update is installing, the MG90's LEDs display an amber 'chase' pattern (LEDs blink in sequence from left to right). For more information on LED patterns, see [LEDs](#) on page 263.

Important: *Do not remove the MG90's power while the LED chase is occurring.*

Note: Boot time increases by 5–6 minutes while installation is in progress.

14.3 Forcing an OTA Update

To manually force an OTA update with AMM:

1. Go to General > Tools:

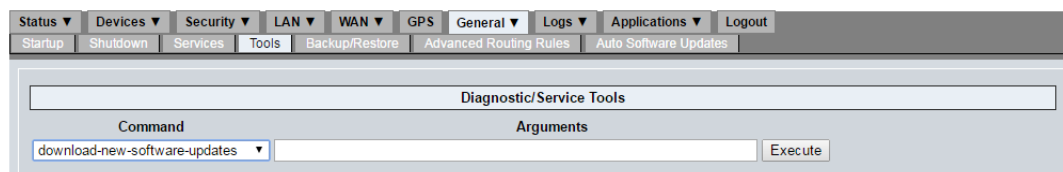


Figure 14-2: Accessing the Diagnostic/Service Tools page

2. In the Command pull-down, select download-new-software-updates.
3. Click Execute. A series of status messages will be displayed.
4. When the message to reboot appears:
 - If the earlier message indicated there were items to be downloaded, press and release the Reset button to reboot the MG90.
 - If the earlier message indicated there was "no upgrade/downgrade ... to be downloaded", there were no software updates available and the MG90 does not have to be rebooted.

14.4 Radio Module Firmware Images

By default, the MG90 automatically manages radio module firmware updates to optimize storage space.

This section describes how to customize the MG90 router's default firmware update behavior and, if needed, manually manage updates and storage.

14.4.1 Firmware Overview

The MG90 ships with certified firmware images for its cellular radio module(s) (MC7354/MC7430/MC7455/EM7511/EM7565/EM9190). These typically include:

- Mobile network provider-specific — Images for certain mobile network providers (for example, in the U.S., AT&T, Verizon, and Sprint)
- Generic — Generic image for other mobile network providers (e.g. T-Mobile, US Cellular, Bell, Telus, Rogers, etc.). The modules are factory-configured with this image.

(Note that some of these providers may also use provider-specific firmwares for some module types.)

These images (and optional other images selected by the user) are stored on the MG90. See [Storing Radio Module Firmware in MG90](#) on page 105 for details.

When the MG90 boots, it checks whether the correct firmware is being used for the installed SIMs (Cellular A uses SIM slots A1 (default) and A2, and Cellular B uses SIM slots B1 (default) and B2). If the SIMs for either cellular radio module require different firmware than the current images, the MG90 will, if SIM-based switching is enabled, install the correct images. See [Firmware Image Switching](#) on page 109 for details. While the new firmware image is installing on the modem, the MG90's LEDs display a green 'chase' pattern (each LED will blink in sequence from left to right).

Note: The boot time will increase by 5–6 minutes while the installation is in progress.

Important: Do not remove the MG90's power while the LED chase is occurring.

Important: Do not replace SIMs while the MG90 is powered on. Power off the MG90, replace the SIM(s), then power on.

When necessary, one or more of the images stored on the MG90 can be purged (deleted) from the device to make space for newer images. See [Purging Firmware Images](#) on page 112 for details.

14.4.2 Storing Radio Module Firmware in MG90

The MG90 can store up to 320 MB of radio module firmware images. These images are listed in the Radio Module Firmware Available section, and any stored images that are currently running on the cellular radio module(s) include an indicator (module location — CA, CB) in the Active column.

Note: The status values 'Uploaded' and 'Available' indicate stored firmware images that were pulled from AMM ('Available') or manually loaded ('Uploaded'), and are available for use. The status 'Requested' label indicates firmware images that have been selected to download from AMM and are not yet available for use.

Radio Module Firmware Options

Firmware Upgrade Option: Upgrade Active

Firmware Upgrade on High Cost Link: ☐

SIM-based Switching Enabled on CA: ☒

SIM-based Switching Enabled on CB: ☒

Radio Module Firmware Available

Active	Status	Module	Carrier	Firmware Version	Size (MB)	Upgrade Disabled	Force Firmware	Purge
	Available	EM7511	ATT	SWI9X50C_01.07.02.00_ATT_002.008_004	80	☐	None	Never
CA	Available	MC7455	VZN	SWI9X30C_02.30.01.01_VERIZON_002.052_001	65	☐	None	Never
	Uploaded	MC7354	BELL	SWI9X15C_05.05.58.00_Bell_005.024_000	35	☐	None	Never
	Available	MC7455	GENERIC	SWI9X30C_02.30.03.00_GENERIC_002.046_001	65	☐	None	Never
	Requested	MC7430	DOCOMO		65	☐	None	Never

Add Firmware

Remaining Disk Space (MB): 10

EM7511 ATT Add

To Upload... Choose and Upload a File From Your Computer

Radio Module Current Status

Cellular CA		Cellular CB	
RM:	UNKNOWN	RM:	UNKNOWN
SIM:	GENERIC	SIM:	ATT
SIM ICCID:	8912230000308943869	SIM ICCID:	89014104254016784715
SIM IMSI:	302220021141991	SIM IMSI:	310410401678471

Figure 14-3: Radio Module Firmware Available example

At any time, firmware images can be stored on the MG90 for future use as long as space is available — the total space remaining for loading new images is shown in the Add Firmware section.

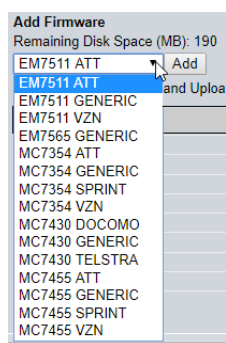
Firmware images can be loaded from the AMM (see [Loading an image from AMM](#) on page 106) or from the computer (see [Loading a signed image from Computer](#) on page 106).

If space is needed to store new images, images in the Radio Module Firmware Available list can be purged — see [Purging Firmware Images](#) on page 112 for details.

14.4.2.1 Loading an image from AMM

To load an officially supported firmware image using AMM:

1. Select a firmware image from the Add Firmware dropdown list, which shows all firmware images officially supported for the MG90. (The following image is an example only.)



The selected firmware is added to the Radio Module Firmware Available list and the Status appears as Requested.

Note: At this point, you can select the requested firmware's Purge NOW option if you made a mistake and do not want to store the image.

2. Click Submit, the firmware begins downloading to the device. When it finishes, a prompt will indicate to reboot to get the requested firmware(s).
3. Reboot the MG90 to install the downloaded firmware on the router. The status of the firmware in the Radio Module Firmware Available list will appear as 'Available'.

14.4.2.2 Loading a signed image from Computer

In certain cases, pre-release or custom firmwares are made available to customers as Signed Firmware Packages (.sfpkg). The firmwares must be loaded to the MG90 from your computer.

To load a signed image that is stored on your computer ('user-managed'):

1. Select a firmware image:
 - a. Click To Upload to display the Signed Firmware Package (SFPKG) Upload screen.

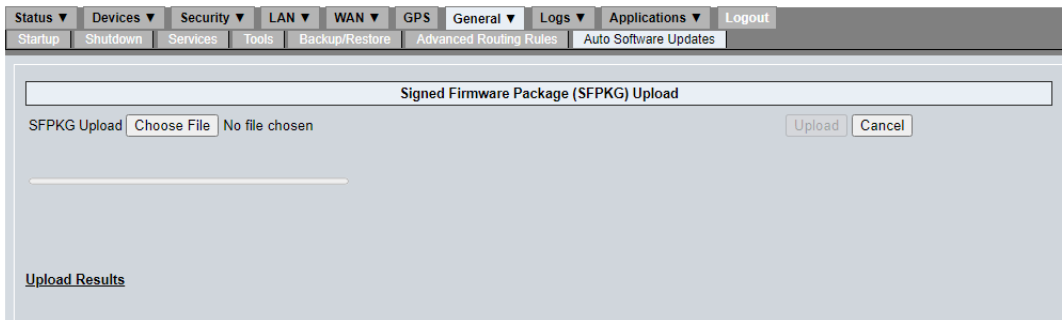


Figure 14-4: Auto Software Updates—Signed Firmware Package Upload

- b. Click Choose File to find the image on the computer, then click Open.
The selected firmware name appears beside the Choose File button.
2. Click Upload. A status message displays the upload progress (% uploaded, then Processing) and then the Upload Results displays the upload log messages.

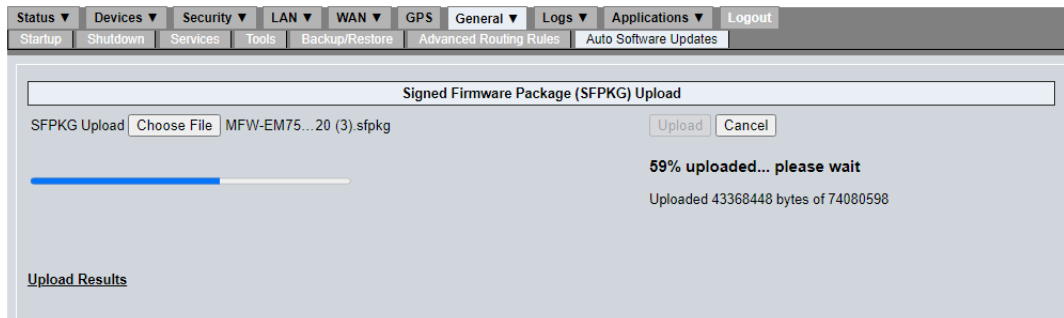


Figure 14-5: Signed Upload—Uploading in progress

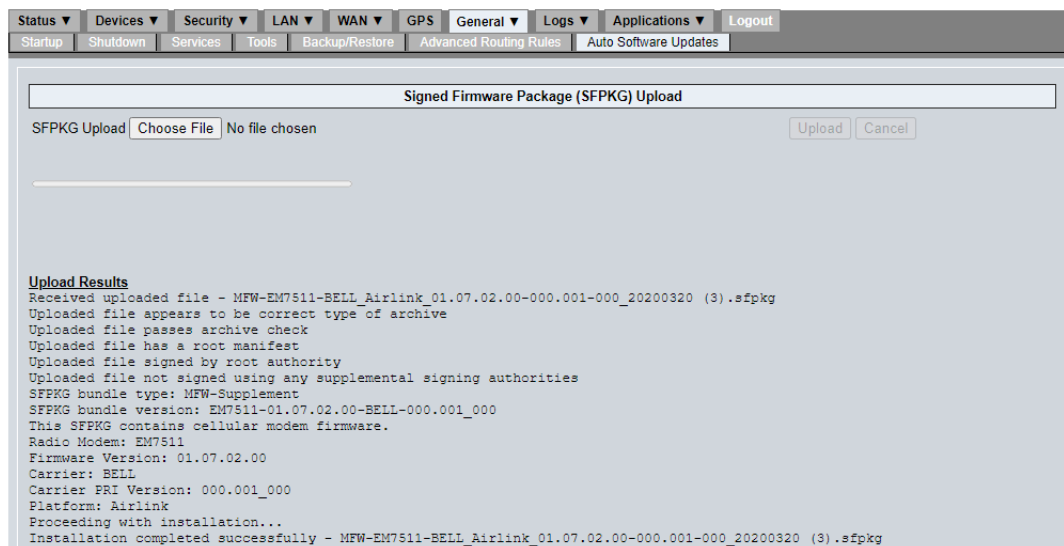


Figure 14-6: Signed Upload—Upload complete

If the image uploaded successfully, the firmware status in the Radio Module Firmware Available list will appear as 'Uploaded'. (No reboot is required.)

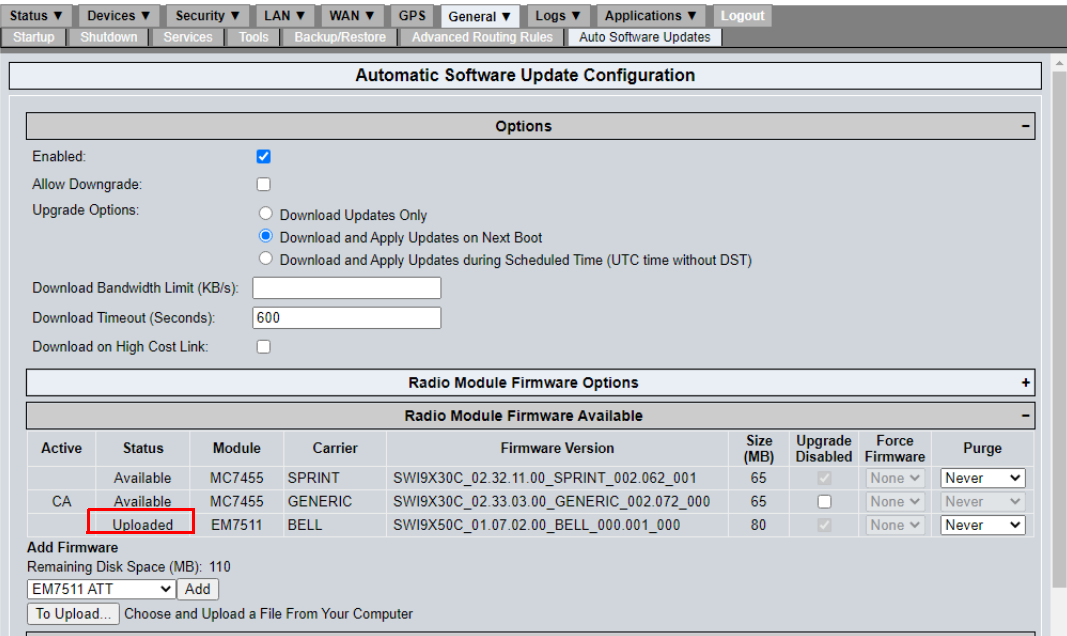


Figure 14-7: Signed Upload — Upload complete

Note: User-managed ('Uploaded') images will not be upgraded when an MGOS upgrade occurs — only AMM-managed ('Available') images will be upgraded.

Important: MGOS will not allow firmware to be loaded on a mismatched radio module type (e.g. MC7354 firmware will not load on an EM7511). However, it will not prevent firmware that is not carrier-certified to run on the MG90 from being loaded. For example, a non-supported EM7511 firmware (something other than AT&T, Verizon, Sprint, or Generic) can be uploaded with To Upload and applied to an EM7511).

14.4.3 Automatic Firmware Upgrades

By configuring the firmware upgrade option and the SIM-based switching option(s), radio module firmware images stored in the MG90 can be automatically upgraded when new versions are available in AMM. Firmware images that are uploaded locally via the LCI will not be automatically upgraded.

Based on the selected upgrade options, when a firmware upgrade is required for an image in the Radio Module Firmware Available list, the MG90 can automatically download from AMM. If the MG90 does not have enough space to store the upgraded image in the Radio Module Firmware Available list, space can be made available (if possible) by purging other images from the list. See [Purging Firmware Images](#) on page 112 for details.

To enable/disable automatic firmware upgrades:

1. Go to General > Auto Software Updates.

Note: The screen appears in 'collapsed' view. To expand or collapse any section (to view or hide its fields), click anywhere on the section's heading bar.

2. Expand the Radio Module Firmware Options section (click anywhere in the section heading).

3. Select a Firmware Upgrade Option:

- Upgrade Active — Allow automatic upgrades of AMM-managed firmware images if they are stored on the MG90 *and* running (Active) on one or more cellular radio modules.

Note: An upgrade image for an active module will only be downloaded from AMM if SIM-Based Switching Enabled is selected for that module, or if the Force Firmware option for an image is set for that module (e.g. 'CA' or 'CB', or 'Both').

- Upgrade All — Allow automatic upgrade of all AMM-managed images stored on the MG90.

Note: If an Active image (an image running on a module) is not stored in the MG90's Radio Module Firmware Available list but should be upgraded, make sure SIM-based Switching Enabled is selected for that module.

- Disabled — Do not allow automatic firmware upgrades.

Note: If Firmware Upgrade is disabled, other firmware options can still be configured, but firmware upgrades will not be done, and the Add Firmware 'Add' button is disabled.

4. By default, Firmware Upgrade on High Cost Link is not selected, so firmware upgrades occur only on low cost links. If you select this option, firmware upgrades can also occur over high cost links.

Note: Firmware Upgrade on High Cost Link can only be selected/de-selected if Download on High Cost Link is selected.

5. If any specific images in the Radio Module Firmware Available list must not be upgraded, regardless of the Firmware Upgrade option, select Upgrade Disabled for each specific image.

6. Click Submit.

14.4.4 Firmware Image Switching

If firmware upgrades are enabled (Active or All) and SIM-based Carrier Switching is enabled, the MG90 compares the firmware images running on the cellular radio modules against the inserted SIM(s) on boot up. If different images are required (e.g. an AT&T SIM is inserted in SIM slot A1 and the current image is intended for Verizon), the MG90 will attempt to automatically 'switch' the image (install the appropriate firmware on the module).

If SIM-based switching is not enabled, module firmware can be installed by manually 'forcing' a firmware switch.

Note: If an image switch occurs for either reason (SIM-based or manually forced switch) and the Firmware Upgrade Option is "Upgrade Active", the Upgrade Disabled checkbox for the now-active firmware is automatically cleared.

14.4.4.1 SIM-based Carrier Switching

SIM-based carrier firmware switching can be enabled on a 'per-module' basis (e.g. Switching can be enabled for CA, CB, or Both.)

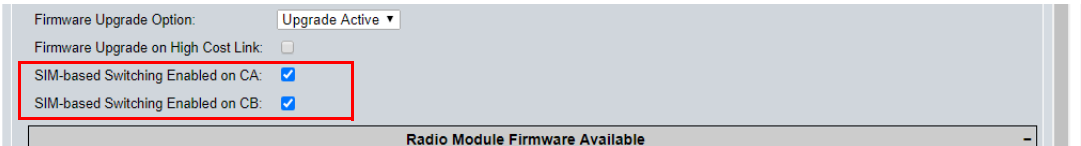
Note: If SIM-based switching is enabled for a given radio module, the Force Firmware option is disabled for corresponding images in the Radio Module Firmware Available list.

To enable SIM-based carrier firmware switching:

1. Go to General > Auto Software Updates.

Note: The screen appears in 'collapsed' view. To expand or collapse any section (to view or hide its fields), click anywhere on the section's heading bar.

2. Expand the Radio Module Firmware Options section (click anywhere in the section heading).
3. Select SIM-based Switching Enabled on Cn for each module that should support switching.



4. Click Submit.

If switching is enabled for a radio module and an image switch is required (determined when the MG90 boots), an appropriate image will be selected from the MG90's stored images. If none is available, the correct image is automatically downloaded from AMM (see [Automatic Firmware Upgrades](#) on page 108 for details).

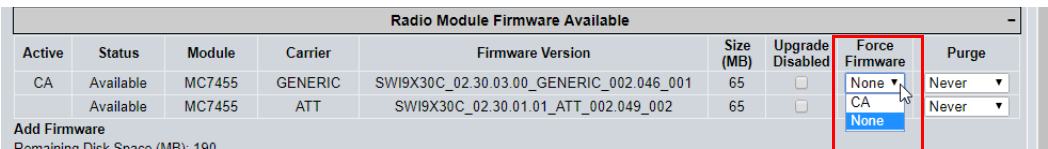
If there is not enough space for the new image on the MG90, one or more images in the Radio Module Firmware Available list will be purged to create space. See [Purging Firmware Images](#) on page 112 for details.

14.4.4.2 Manual Firmware Switching (Forcing a Switch)

If SIM-based carrier switching is disabled for a cellular radio module, the MG90 will not automatically switch the firmware to match the carrier.

To manually switch the firmware for radio module(s) that do not have SIM-based carrier switching enabled:

1. In the Radio Module Firmware Available section, select CA, CB, or Both from the Force Firmware list for the firmware to be loaded on the radio module(s). (Available options depend on the number of radio modules.)



Note: If Force Firmware is enabled for a given module, the corresponding SIM-based Switching Enabled option is disabled in the Radio Module Firmware Options section.

Note: When a module is selected in the Force Firmware field for one image, that module will not be selectable for any other image. To choose a different firmware image to force to the module, reset the first image's Force Firmware option to None (or a different module), and then set the new image's Force Firmware correctly.

2. Click Submit.
The selected firmware will be installed to the specified radio modules the next time the MG90 boots.

14.4.4.3 Image Switching Process

The image switching process, and the options that may affect its success, are shown in [Figure 14-8](#), below.

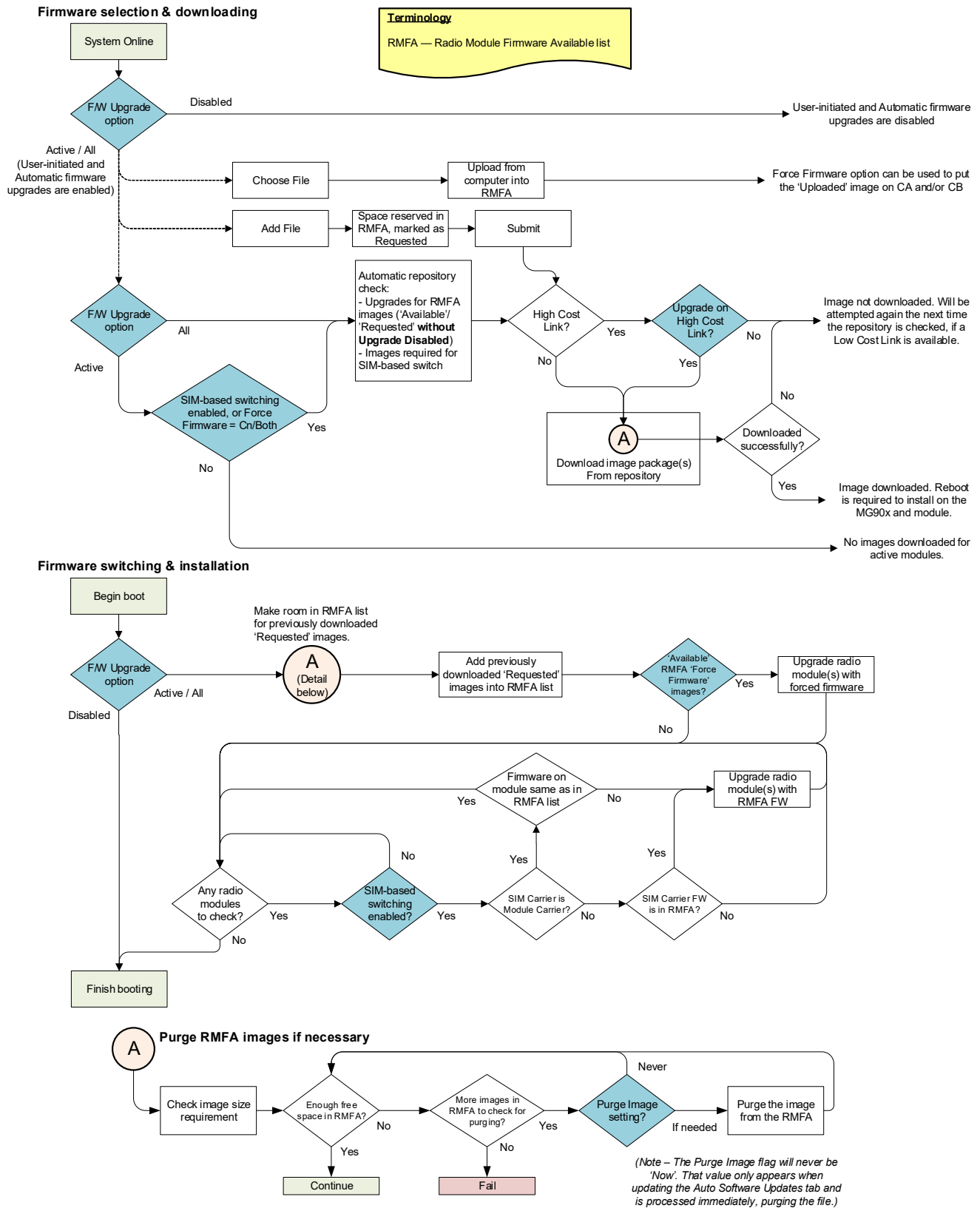


Figure 14-8: Firmware Upgrade and Switching Processes

While the new firmware image is installing on the modem, the MG90's LEDs display a green 'chase' pattern (each LED will blink in sequence from left to right). When the installation finishes, the LEDs return to their normal behavior. (See [LEDs](#) on page 263 for details).

14.4.5 Purging Firmware Images

Once firmware images have been stored on the MG90, they remain until they are manually or automatically purged (deleted) to make room for different or upgraded images. The Purge flag associated with each image in the Radio Module Firmware Available controls the image can be purged:

- If needed — Automatic purging. During the boot process, if space is needed to install a new image due to a SIM-based switch or to install an upgraded image when it becomes available in AMM, the image can be automatically purged.

Images will be purged in the following order:

- Sprint
- AT&T
- Telstra
- Generic
- Verizon
- User-managed firmware (firmware from the Source, custom-built, etc.)
- Now — Manual purging. When selected the image is flagged for purging. The Size changes to 0 (indicating the file will be purged), and the Remaining Disk Space increases to include the space that will be freed.

Important: *If 'Now' is selected, the image purges as soon as Submit is clicked.*

- Never — Default. Image will not be purged.

For detailed information, see [General > Auto Software Updates](#) on page 247.

To configure firmware image file purging:

1. Go to General > Auto Software Updates.

Note: The screen appears in 'collapsed' view. To expand or collapse any section (to view or hide its fields), click anywhere on the section's heading bar.

2. Expand the Radio Module Firmware Available section (click anywhere in the section heading).
3. For each listed image, set the Purge option as appropriate:
 - If needed — Automatically purge during boot sequence if space is needed for a firmware upgrade or SIM-based image switch.
 - Now — Purge image when Submit is clicked.
 - Never — Purging disabled
4. Click Submit.
5. A prompt will appear if any images are marked to purge 'Now', indicating that purging will take several minutes. Click OK and wait until the screen redisplay with updated information.

14.4.6 Listing Firmware Images

Information about the firmware images installed on the MG90 and running on its cellular radio modules is available in the following locations:

- Auto Software Updates (General > Auto Software Updates)

- Images stored on the MG90 — Listed in the Radio Firmware Available section
- Images running on cellular radio modules — Indicated in the Radio Firmware Available section's Active field, and shown with other module information in the Radio Module Current Status section
- WAN General Information (Status > General)
 - Listed with version numbers only

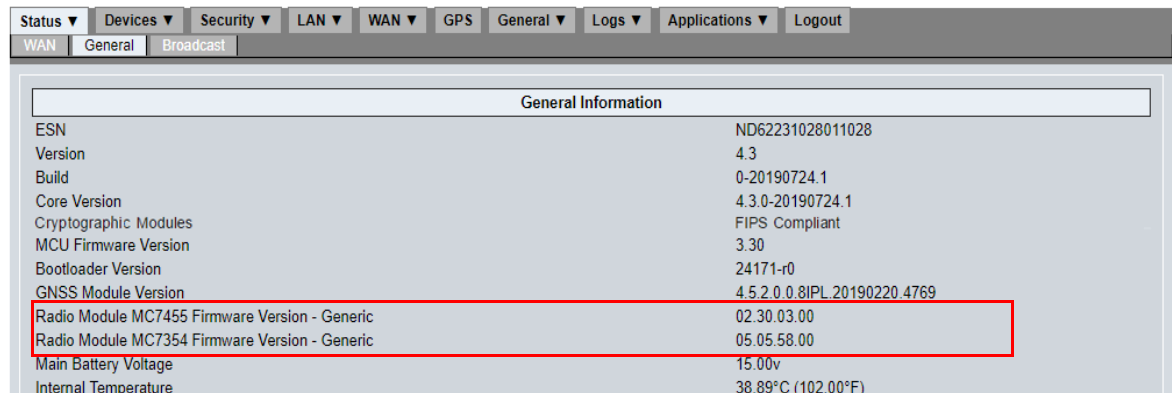


Figure 14-9: Viewing the Available Radio Module Firmware Image Packages

- Extended WAN Link Status (Status > WAN > Show Extended Status)
 - Listed in the Cellular Info section for each active radio module

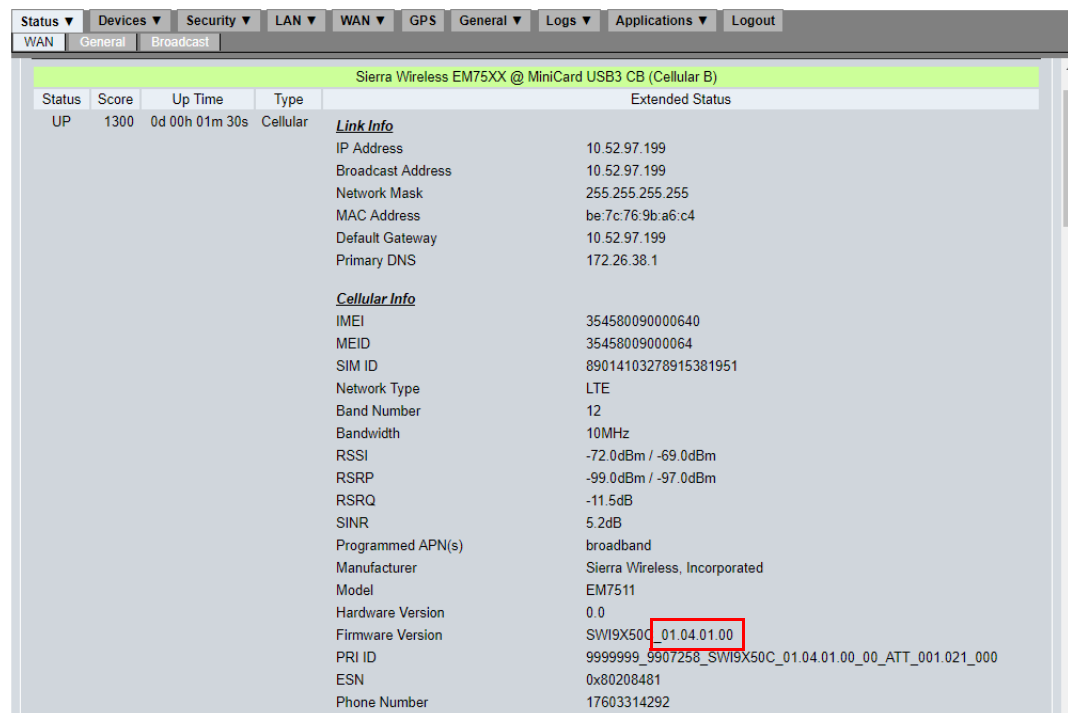


Figure 14-10: Viewing Installed Radio Module Firmware

A: Status Tab

This chapter describes the Status tab, which displays information about connected WAN devices, and details of the MG90's current hardware and software status.

The Status tab includes the following sub-tabs:

- WAN — Status of all links (devices) that are currently configured for WAN access. See [WAN Link Status Tab](#) on page 114.

Note: WAN Link Status is the first screen that appears when you log in to the LCI.

- General — MG90 hardware and software details. See [General Information](#) on page 120.
- Broadcast — Status Broadcast options. See [Status Broadcast](#) on page 123.

A.1 WAN Link Status Tab

The WAN Link Status tab (Status > WAN) displays summary information when the screen appears, and extended (detailed) information when Show Extended Status is selected.

A.1.1 Summary status screen

The summary WAN Link Status screen lists all devices (links) that are currently configured for WAN access, and their connection status. The currently active link is highlighted in green as shown in [Figure A-1](#).

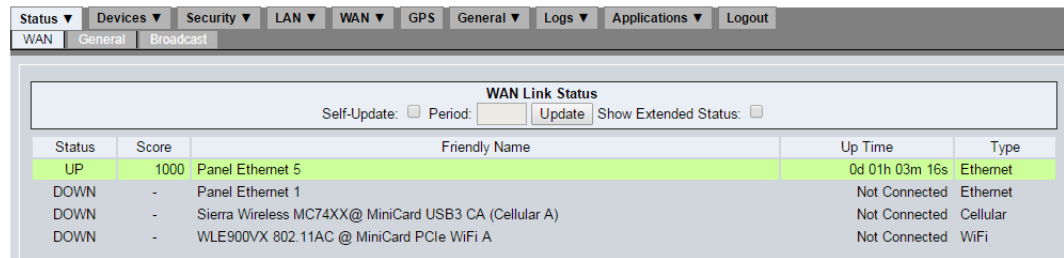


Figure A-1: WAN Link Status summary screen (Status > WAN)

Table A-1: WAN Link Status (Summary) screen fields / buttons

Field / Button	Description
Self-Update	Select to make the screen automatically refresh every <Period> seconds.
Period	Number of seconds between automatic screen refreshes (when Self-Update is selected). - Valid range: 5–99. (Note — If you enter 0–4, the value rounds up to 5 automatically.) - Other values — Ignored
Update (button)	Click to refresh the screen.
Show Extended Status	Select to display detailed information about the WAN links. See Extended status screen on page 115.

Table A-1: WAN Link Status (Summary) screen fields / buttons (Continued)

Field / Button	Description
Status	Current state of the WAN link - UP — Link is connected - DOWN — Link is not connected <i>Note: More than one link can be UP at the same time. The active link is highlighted in green.</i> If you want to stop the currently active link from carrying traffic, either temporarily set its status to IDLE (e.g. in Devices > Cellular), or fine-tune its policies to adjust its score (see Setting up WAN Link Policies on page 51.)
Score	Priority score used to dynamically determine which WAN link will be used The MG90 tries to use the link with the highest score as the active link. For details on configuring links to dynamically change based on connection status, geographic location, time of day, etc., see Setting up WAN Link Policies on page 51.
Friendly Name	Descriptive name for the WAN link To change the description, see the Devices Tab on page 126.
Up Time	Connection duration - UP link — Amount of time the link has been connected for current session. - DOWN link — “Not Connected”
Type	WAN link type - Cellular — An LTE/5G radio installed in the MG90. - Ethernet — One of the Ethernet ports on the MG90’s back panel. - Wi-Fi — A Wi-Fi radio installed in the MG90. - Serial modem — An optional Harris Land Mobile Radio connected to the MG90’s serial port.

A.1.2 Extended status screen

The extended WAN Link Status screen lists all devices (links) that are currently configured for WAN access, and configuration details and traffic data for each link. The currently active link is highlighted in green as shown in [Figure A-2](#).

Note: This screen is read-only, none of the information displayed can be updated from this screen.

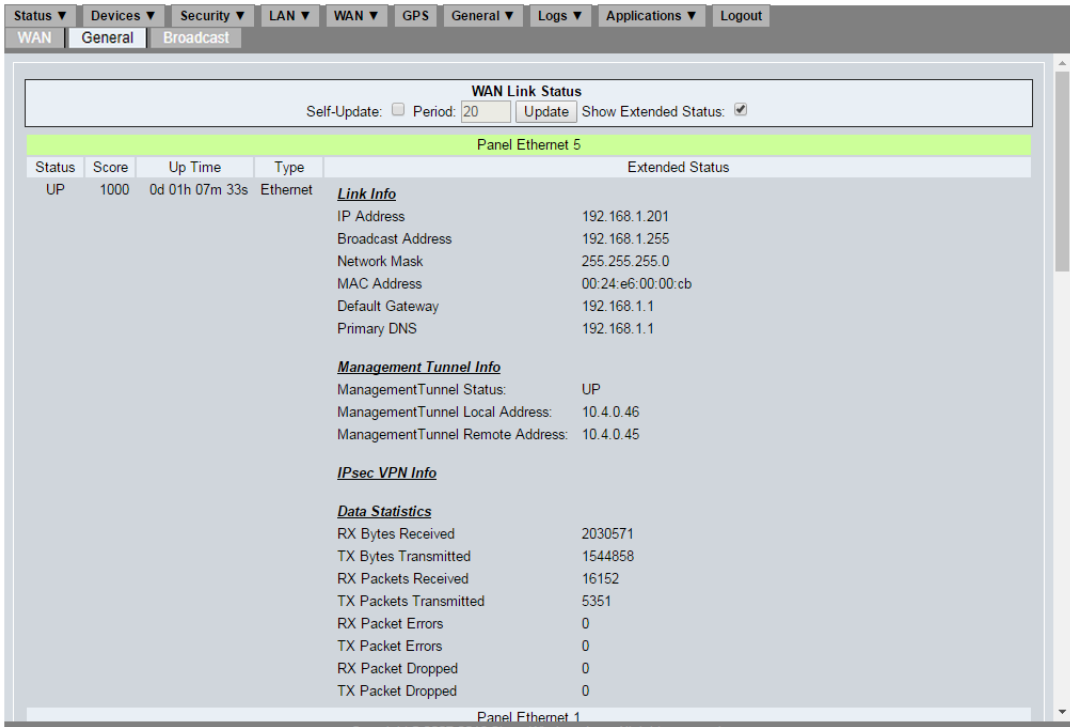


Figure A-2: WAN Link Status extended screen (Status > WAN > Extended Status)

Table A-2: WAN Link Status (Extended) screen fields

Field	Description
Status	Current state of the WAN link - UP — Link is connected - DOWN — Link is not connected <i>Note: More than one link can be UP at the same time. The active link is highlighted in green.</i> If you want to stop a link from carrying traffic link, either: - Set the link's status to IDLE (e.g. in Devices > Cellular), or - Fine-tune the link's policies so its scores will adjust appropriately. (See Setting up WAN Link Policies on page 51.)
Score	Priority score used to dynamically determine which WAN link will be used The MG90 tries to use the link with the highest score as the active link. To configure links to dynamically adjust their scores based on connection status, geographic location, time of day, etc., see Setting up WAN Link Policies on page 51.
Up Time	Connection duration - UP link — Amount of time the link has been connected for current session. - DOWN link — "Not Connected"

Table A-2: WAN Link Status (Extended) screen fields (Continued)

Field	Description
Type	WAN link type: - Cellular — LTE/5G radio installed in the MG90. - Ethernet — One of the Ethernet ports on the MG90's back panel. - Wi-Fi — Wi-Fi radio installed in the MG90. - Serial modem — Optional Harris Land Mobile Radio connected to the MG90's serial port.
Extended Status	Detailed information about the WAN link, including configuration, link, and performance data. The information displayed depends on the type of WAN Link (Cellular, Ethernet, or Wi-Fi).
Link Info (appears only for Cellular or Ethernet WAN devices)	
IP Address	IPv4 address assigned to the link Example: 192.168.1.201
Broadcast Address	IPv4 address of the subnet that the link is part of
Network Mask	Network mask assigned to the link
MAC Address	MAC address of the link
Default Gateway	IPv4 address of the gateway that assigned the link's IP Address
Primary DNS	Mobile Network Operator's DNS IP Address
Secondary DNS Servers	IPv4 addresses of the mobile network operator's secondary DNS servers
Cellular Info (appears only for Cellular WAN devices)	
IMEI	Cellular device's unique International Mobile Equipment Identity code
MEID	Cellular device's unique Mobile Equipment Identifier
SIM ID	Identification number for the SIM card in use
SIM Type	FirstNet — Indicates a FirstNet SIM is installed. <i>Note: Field appears only if a FirstNet SIM is installed.</i>
Network Type	Type of network the gateway is connected to - CDMA - EVDO - GSM - HDR - HSPA - LTE - WCDMA 1XRTT - ENDC
Band Number	Current cellular band being used
Bandwidth	Bandwidth of current cellular band

Table A-2: WAN Link Status (Extended) screen fields (Continued)

Field	Description
SCC1 SCC2 SCC3 SCC4	Secondary Component Carrier (SCC) carrier aggregation status details Formats: - State: <state> Band: <band> BW: <bw> Channel: <channel> - State: Not Assigned Parameters: <state> — CA state: - Active — CA available and the SCC is being used - Inactive — CA available, SCC is not currently passing traffic - Not Assigned — SCC is not assigned for CA <band> — LTE band <bw> — Bandwidth <channel> — Channel number <i>Note: Fields appear only for cellular devices that support carrier aggregation. (i.e., radio modules (EM9190, EM7511/EM7565, MC7430/MC7455))</i>
<i>Note: For cellular devices that support carrier aggregation (i.e., radio modules (EM9190, EM7511/EM7565, MC7430/MC7455)), the fields below (RSSI, RSRP, RSRQ, and SINR) are for the Primary Component Carrier (PCC).</i>	
RSSI	LTE Received Signal Strength Indicator
RSRP	LTE Reference Signal Received Power (signal power)
RSRQ	LTE Reference Signal Received Quality
SINR	LTE Signal-to-interference-plus-noise ratio (SINR level)
<i>Note: The '5G NR' fields below (5G NR Band Number to 5G NR SINR) appear only for EM9190 radio modules.</i>	
<i>Note: The 5G NR Bandwidth, 5G NR RSRP, 5G NR RSRQ, and 5G NR SINR fields are for the Primary Component Carrier (PCC).</i>	
5G NR Band Number	Current 5G band being used <i>Note: If the module is configured for 2x2 MIMO, a message indicates band n41 is not available.</i>
5G NR Bandwidth	Bandwidth of current 5G band
5G NR RSRP	5G Reference Signal Received Power (signal power)
5G NR RSRQ	5G Reference Signal Received Quality
5G NR SINR	5G Signal-to-interference-plus-noise ratio (SINR level)
Programmed APN(s)	APN(s) that are pre-programmed in the radio module
Manufacturer	Name of the cellular device's manufacturer (i.e. "Sierra Wireless, Inc")
Model	Cellular device's model number
Hardware Version	Cellular device's hardware version number
Firmware Version	Firmware version running on the cellular device
SKU PRI ID, Revision	SKU-specific configuration version <i>Note: Field appears only for radio modules.</i>

Table A-2: WAN Link Status (Extended) screen fields (Continued)

Field	Description
Carrier PRI ID	Carrier-specific configuration version <i>Note: Field appears only for radio modules.</i>
Phone Number	Phone number associated with the SIM card in use
PRL Version	Version number of the Preferred Roaming List issued by the carrier
Roaming Indicator	Roaming state "Home" (i.e., Not roaming) "Roaming"
Service	Service type (e.g. "LTE", "UMTS")
MTU	Maximum Transmission Unit
Provision Status	"Provisioned" or "Not Provisioned" <i>Note: Sprint-only field, does not appear for other carriers.</i>
Wi-Fi Info (appears only for Wi-Fi WAN devices)	
WPA State	Wi-Fi connection state: - COMPLETED - DISCONNECTED
Band	802.11 network access control protocol version
SSID	Basic Service Set Identifier The identifier that appears to a device when it scans for access points.
Mode	802.11 operation mode - adhoc — This option is used only when the AP that the link is connected to is using WEP. - Managed — Default
Frequency	Wi-Fi frequency
Access Point	Wi-Fi device's MAC address
Link Quality	Wi-Fi signal quality Signal-to-noise ratio determined by various link parameters, including Bit Error Ratio (BER) and Signal, Noise and Distortion (SINAD). Example: 70/70
Signal Level	Wi-Fi signal strength, in dBm
Management Tunnel Info	
Management Tunnel Status	Status of management tunnel (secure VPN that AMM can use to access MG90) - UP - DOWN

Table A-2: WAN Link Status (Extended) screen fields (Continued)

Field	Description
Management Tunnel Local Address	IPv4 addresses relating to the management tunnel When a WAN link is established, the MG90 sends a request to the AMM Server Address to initiate the tunnel. The MG90 establishes its end of the tunnel at the Local Address and AMM establishes its end at the Remote address. The Gateway Address is the private network address of the server on the MG90 that hosts the tunnel. - Local Address — Address of the MG90 end of the tunnel, issued by the VPN server. - Remote Address — Address of the AMM end of the tunnel. (AMM Tunnel IP Address specified in Table E-15 on page 202.) - Gateway Address — IP address of the VPN server on AMM. - Server Address — Public address of the AMM server.
Management Tunnel Remote Address	
Management Tunnel Gateway Address	
Management Tunnel Server Address	
Management Tunnel Server Port	Port that the tunnel is using on the AMM server. (The AMM server will have multiple ports available.) <i>Note: This value appears only when the tunnel is up.</i>
IPsec VPN Info (Details repeat for each defined VPN associated with the device)	
IPsecVPN 1 Name	VPN descriptive name This is the Friendly Name field from the IPsec VPN Configuration screen.
IPsecVPN 1 Status	VPN status - UP - DOWN
IPsecVPN 1 Local Address	VPN gateway IP address This is the Server Address Field from the IPsec VPN Configuration screen.
Data Statistics	
RX Bytes Received	Total number of bytes received from the network since the link became active
TX Bytes Transmitted	Total number of bytes transmitted to the network since the link became active
RX Packets Received	Total number of packets received from the network since the link became active
TX Packets Transmitted	Total number of packets transmitted to the network since the link became active
RX Packet Errors	Number of packets received with errors since the link became active
TX Packet Errors	Number of packets transmitted with errors since the link became active
RX Packet Dropped	Number of received packets dropped since the link became active
TX Packet Dropped	Number of transmitted packets dropped since the link became active

A.2 General Information

The General Information screen (Status > General) displays basic details about the MG90's hardware, operating software, and GPS details, as shown in [Figure A-3](#).

Note: This screen is read-only, none of the information displayed can be updated from this screen.

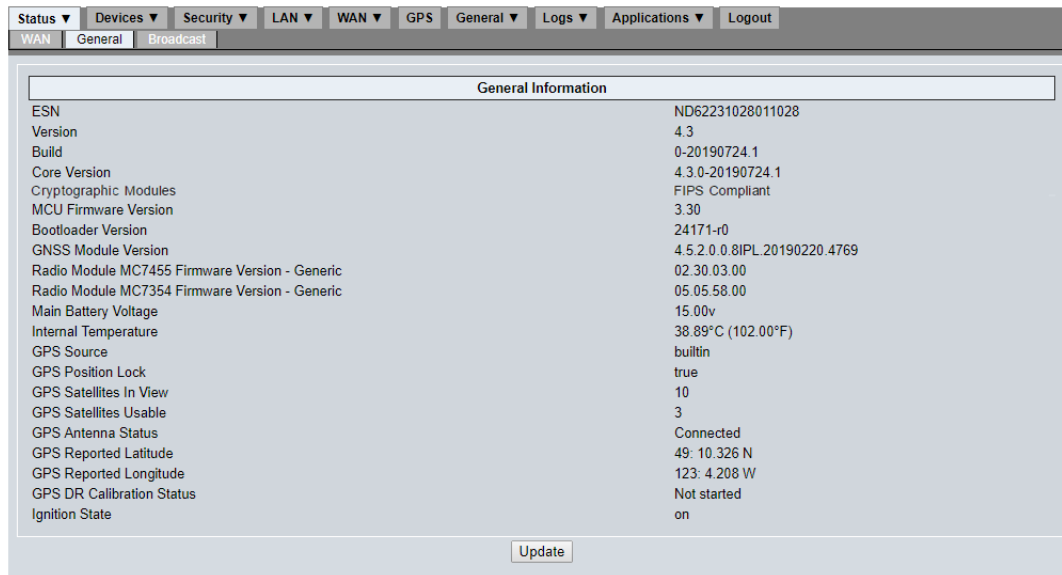


Figure A-3: General Information screen (Status > General)

Table A-3: General Information screen fields

Field	Description
ESN	MG90 serial number <i>Note: The ESN is also printed on a label on the bottom of the MG90.</i>
Version	Main version number
Build	Hardware build version
Core Version	Software version number
Cryptographic Modules	Indicates the router is "FIPS Compliant". This appears only if the MG90 is configured for FIPS.
MCU Firmware Version	MCU firmware version number
Bootloader Version	Bootloader version number
GNSS Module Version	GNSS module version number
Radio Module <type> Firmware Version <fw_type>	Cellular module firmware versions present on the MG90.
Main Battery Voltage	Power supply voltage (Vehicle battery, AC power supply, etc.)
Internal Temperature	MG90 device's internal temperature

Table A-3: General Information screen fields (Continued)

Field	Description
GPS Source	Device type providing GPS functionality: ▪ builtin — The internal GPS device included with the MG90. ▪ ethernet — GPS device connected to an Ethernet port. ▪ serial — GPS device connected to the serial port (DB-9 connector).
GPS Position Lock	Status of the GPS fix: ▪ false — No GPS fix ▪ true — GPS fix acquired <i>Note: Four or more satellites must be found to get a position lock.</i>
GPS Satellites In View	Number of satellites detected by the GPS device
GPS Satellites Usable	Number of satellites usable by the GPS device
GPS Antenna Status	Current status of GPS antenna connector on MG90's rear panel: ▪ Connected ▪ Disconnected
GPS Reported Latitude	Last reported GPS fix position
GPS Reported Longitude	
GPS DR Calibration Status	Status of Dead Reckoning calibration process ▪ Not started ▪ In progress ▪ Complete
Ignition State	Vehicle ignition state: ▪ on ▪ off

A.3 Status Broadcast

The Status Broadcast Configuration screen (Status > Broadcast) allows broadcasting of selected MG90 status information over UDP. This feature can be enabled/ disabled and customized as shown in [Figure A-4](#).

Status Broadcast Configuration	
Options	
Enable	☐
Broadcast Port	21010
LAN Segments	☒ Default LAN 172.22.0.1 ☒ LAN-1 172.22.1.1 ☐ LAN-2 172.22.2.1
Broadcast on Time Interval	☒
Broadcast Interval (ms)	60000
Broadcast on GPIO State Change	☐
GPIO Sampling Interval (ms)	10000
Broadcast on WAN State Change	☐
WAN Sampling Interval (ms)	10000
Broadcast Data	
Location	☒
GPIO States	☒
WAN States	☒
WAN Network Type	☒
WAN Signal Strength	☒
Cellular Band Number	☒
Cellular Bandwidth	☒
Cellular RSSI	☒
Cellular RSRP	☒
Cellular RSRQ	☒
Cellular SINR	☒
5G NR Band Number	☒
5G NR Bandwidth	☒
5G NR RSRP	☒
5G NR RSRQ	☒
5G NR SINR	☒
GNSS Status:	
GPS Fix	☒
Number of Satellites	☒
GPS Antenna Connected	☒
VPN Status	☒
☒ Combined	
☐ Individual	
General Status:	
Ignition Status	☒
Main Battery Voltage	☒

Figure A-4: Status Broadcast Configuration screen (Status > Broadcast)

Table A-4: Status Broadcast Configuration screen fields

Field	Description
Options	
Enable	Status Broadcast state: - Selected — Enabled. Status details will broadcast at the specified Broadcast Interval, GPIO Sampling Interval (if state changes occur), or both. - Not selected — Disabled <i>Note: One or both of Time Interval Mode and GPIO State Change Mode must be selected.</i>
Broadcast Port	UDP port to use for broadcasting
LAN Segments	LAN segments to use for broadcasting
Broadcast on Time Interval	Enable / disable time interval broadcasting
Broadcast Interval (ms)	Broadcast frequency in milliseconds (used for Time Interval Mode only) Minimum: 500 ms
Broadcast on GPIO State Change	Enable / disable broadcasting triggered by GPIO state changes
GPIO Sampling Interval (ms)	GPIO sampling frequency in milliseconds (used for GPIO State Change Mode only)
Broadcast on WAN State Change	Enable / disable broadcasting triggered by WAN link connection status changes
WAN Sampling Interval (ms)	WAN state sampling frequency in milliseconds (used for Broadcast on WAN State Change only)
Broadcast Data	
Location	Include latitude and longitude coordinates
GPIO States	Include input and output states for all five GPIOs
WAN States	Include details for each WAN link: - Friendly name (string) - Status: 0 (link is down) or 1 (link is up) - Active ("true" or "false") Selecting this option also allows additional fields to be selected (listed below, from WAN Network Type to Cellular SINR)
WAN Network Type	"Cellular" "Ethernet" "WiFi"
WAN Signal Strength	Signal strength (RSSI) in dBm of the Cellular or Wi-Fi WAN interface e.g. "-79.7"
Cellular Band Number	3GPP band number e.g. "2" (Band 2)
Cellular Bandwidth	LTE bandwidth (in MHz)

Table A-4: Status Broadcast Configuration screen fields (Continued)

Field	Description
Cellular RSSI	LTE Received Signal Strength Indicator (in dB) Range: -120 to 0
Cellular RSRP	LTE Reference Signal Receive Power (in dBm) Range: -140 to 44
Cellular RSRQ	LTE Reference Signal Receive Quality (in dB) Range: -20 to -3
Cellular SINR	LTE Signal to Interference plus Noise (in dB) Range: -20 to +30
5G NR Band Number	<i>Note: This field is available only for 5G routers.</i> 5G 3GPP band number e.g. "2" (Band 2); "n28" (Band n28)
5G NR Bandwidth	<i>Note: This field is available only for 5G routers.</i> 5G NR bandwidth (in MHz)
5G NR RSRP	<i>Note: This field is available only for 5G routers.</i> 5G Reference Signal Receive Power (in dBm) Range: -140 to 44
5G NR RSRQ	<i>Note: This field is available only for 5G routers.</i> 5G Reference Signal Receive Quality (in dB) Range: -20 to -3
5G NR SINR	<i>Note: This field is available only for 5G routers.</i> 5G Signal to Interference plus Noise (in dB) Range: -20 to +30
GNSS Status	
GPS Fix	Include Fix availability (true or false)
Number of Satellites	Include number of usable satellites
GPS Antenna Connected	Include GPS antenna connected state (true or false)
VPN Status	
Combined	Include VPN status 0 (No VPNs established) or 1 (At least one VPN established)
Individual	Include each VPN's 'Friendly Name' and status (0—Down, 1—Up)
General Status	
Ignition Status	Include vehicle ignition status (true or false)
Main Battery Voltage	Include main battery voltage (in Volts)
Internal Temperature	Include internal MG90 temperature (in °C)

B: Devices Tab

This chapter describes the Devices tab, which is used to configure the devices installed in (or connected to) the MG90 that provide network connectivity.

The Devices tab includes the following sub-tabs:

- Cellular — Display the installed cellular (LTE / 5G) radios, and configure them for WAN use or idle them. See [Devices > Cellular](#) on page 126.
- Ethernet — Display the pre-installed Ethernet ports, and configure them for WAN or LAN use, or idle them. See [Devices > Ethernet](#) on page 127.
- Wi-Fi — Display the installed Wi-Fi radios, and configure them for WAN or LAN use, or idle them. See [Devices > Wi-Fi](#) on page 128.
- Serial Modem — Add an optional Harris Land Mobile Radio, and configure it for WAN use, or idle it. See [Devices > Serial Modem](#) on page 129.
- Serial — Configure the MG90's DB9 serial port for console access or application (external device) use. See [Devices > Serial](#) on page 130.
- Bluetooth — Configure the internal Bluetooth device. See [Devices > Bluetooth](#) on page 131.

B.1 Devices > Cellular

The Cellular devices tab lists the cellular radios that are currently installed in the MG90, and any that were previously installed and have since been removed.

From this tab, you can configure the radios' display names and make them available for WAN connections or idle them.

Note: WAN-enabled radios will appear on the Status > WAN screen.

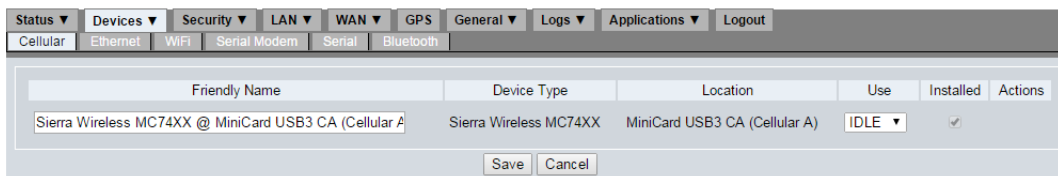


Figure B-1: LCI: Devices > Cellular—Sample screen

Table B-1: Devices > Cellular screen fields

Field	Description
Friendly Name	Enter a descriptive name for the cellular radio. This name identifies the radio in other LCI screens (e.g. Status > WAN).
Device Type	Cellular radio's model name / number
Location	Internal position of the cellular radio For example: - MiniCard USB3 CA (Cellular A) — Uses the Cellular A antenna connectors. - MiniCard USB3 CB (Cellular B) — Uses the Cellular B antenna connectors.

Table B-1: Devices > Cellular screen fields (Continued)

Field	Description
Use	Select the current usage mode of the cellular radio. ■ IDLE — Radio cannot be used for WAN connection at this time. ■ WAN — Radio can be used for a WAN connection. To check its connection status, see WAN Link Status Tab on page 114. To change the usage mode, select a different value and click Save.
Installed	Cellular radio installation status ■ Selected — Radio is installed in the MG90. ■ Not selected — Radio has been removed from the MG90.
Actions	Not applicable

B.2 Devices > Ethernet

The Ethernet devices tab lists the pre-installed Ethernet ports located on the MG90's rear panel.

From this tab, you can configure the ports' display names and make them available for WAN connections, LAN connections, or idle them.

Note: WAN-enabled ports will appear on the Status > WAN screen.

The screenshot shows the 'Devices > Ethernet' configuration screen. At the top is a navigation bar with tabs: Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below this is a sub-bar with tabs: Cellular, Ethernet (selected), WiFi, Serial Modem, Serial, and Bluetooth. The main content area contains a table with the following columns: Friendly Name, Device Type, Location, Use, Installed, and Actions. There are five rows of data, each representing an Ethernet port (Panel Ethernet 1 through 5). Each row has a text input field for the Friendly Name, a dropdown for Device Type (all set to 'Device Built-in Ethernet Port'), a dropdown for Location (all set to 'Panel Ethernet 1' through 'Panel Ethernet 5'), a dropdown for Use (set to 'LAN' for ports 1-3 and 'WAN' for ports 4-5), a checkbox for Installed (all checked), and an 'Actions' column. At the bottom of the table are 'Save' and 'Cancel' buttons.

Friendly Name	Device Type	Location	Use	Installed	Actions
Panel Ethernet 1	Device Built-in Ethernet Port	Panel Ethernet 1	LAN	☒	
Panel Ethernet 2	Device Built-in Ethernet Port	Panel Ethernet 2	LAN	☒	
Panel Ethernet 3	Device Built-in Ethernet Port	Panel Ethernet 3	LAN	☒	
Panel Ethernet 4	Device Built-in Ethernet Port	Panel Ethernet 4	WAN	☒	
Panel Ethernet 5	Device Built-in Ethernet Port	Panel Ethernet 5	WAN	☒	

Figure B-2: LCI: Devices > Ethernet—Sample screen

Table B-2: Devices > Ethernet screen fields

Field	Description
Friendly Name	Enter a descriptive name for the Ethernet port. This name identifies the port in other LCI screens (e.g. Status > WAN and LAN > LAN Segments).
Device Type	All Ethernet ports are listed as "Device Built-in Ethernet Port".
Location	Connector position (1–5) on the MG90's rear panel

Table B-2: Devices > Ethernet screen fields (Continued)

Field	Description
Use	Select the current usage mode of the Ethernet port. ■ IDLE — Port cannot be used for WAN or LAN connection at this time. ■ WAN — Port can be used for WAN connection. To check its current connection status, see WAN Link Status Tab on page 114. ■ LAN — Port can be used to connect a device (such as a notebook) to the MG90's LAN. To change the usage mode, select a different value and click Save.
Installed	Ethernet port installation status ■ Selected — Port is installed in the MG90. ■ Not selected — Port has been removed from the MG90 or is not functioning.
Actions	Not applicable

B.3 Devices > Wi-Fi

The Wi-Fi devices tab lists the Wi-Fi radios that are currently installed in the MG90, and any that were previously installed and have since been removed.

From this tab, you can configure the radios' display names and make them available for WAN connections, LAN connections (acting as an access point for other devices), or idle them.

Note: WAN-enabled Wi-Fi radios will appear on the Status > WAN screen.

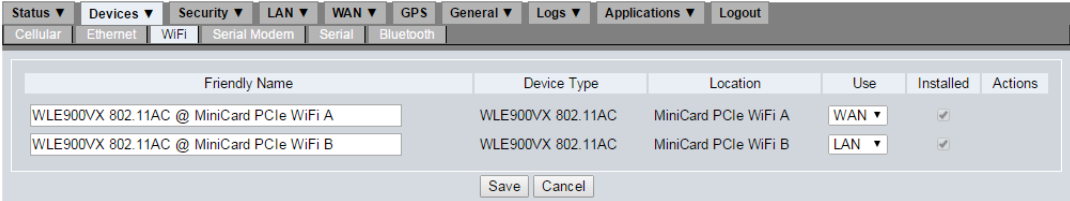


Figure B-3: LCI: Devices > Wi-Fi— Sample screen

Table B-3: Devices > Wi-Fi screen fields

Field	Description
Friendly Name	Enter a descriptive name for the Wi-Fi radio. This name identifies the radio in other LCI screens (e.g. Status > WAN and LAN > LAN Segments).
Device Type	Wi-Fi radio's model name
Location	Internal position of the Wi-Fi radio: ■ MiniCard PCIe Wi-Fi A — Uses the Wi-Fi A antenna connectors. ■ MiniCard PCIe Wi-Fi B — Uses the Wi-Fi B antenna connectors.

Table B-3: Devices > Wi-Fi screen fields (Continued)

Field	Description
Use	Select the current usage mode of the Wi-Fi radio. ▪ IDLE — Wi-Fi radio cannot be used for WAN or LAN connections at this time. ▪ WAN — Wi-Fi radio can be used for a WAN connection. To check its current connection status, see WAN Link Status Tab on page 114. ▪ LAN — Wi-Fi radio can be used as an access point to provide LAN connections for other devices (such as notebooks, smartphones, etc.). To change the usage mode, select a different value and click Save.
Installed	Wi-Fi radio installation status ▪ Selected — Radio is installed in the MG90. ▪ Not selected — Radio has been removed from the MG90.
Actions	Not applicable

B.4 Devices > Serial Modem

If a serial modem (Harris Land Mobile Radio) is used with your MG90, it appears on the Serial Modem device tab.

From this tab, you can configure the serial modem's display name and make it available for a WAN connection, or temporarily idle it.

Note: A WAN-enabled serial modem will appear on the Status > WAN screen.

The screenshot shows the 'Serial Modem' configuration screen. At the top, there are tabs for Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below these are sub-tabs for Cellular, Ethernet, WiFi, Serial Modem, Serial, and Bluetooth. The main area contains a table with the following data:

Friendly Name	Device Type	Location	Use	Actions
My Harris Land Mobile Radio	TTY Serial Port	Serial Port Panel Tx/Rx (LPUART1)	WAN	

At the bottom of the table, there are 'Save' and 'Cancel' buttons.

Figure B-4: LCI: Devices > Serial Modem—Sample screen

Table B-4: Devices > Serial Modem screen fields

Field	Description
Friendly Name	Enter a descriptive name for the serial modem device. This name identifies the device in other LCI screens (e.g. Status > WAN).
Device Type	The MG90 supports the Harris Land Mobile Radio as a serial modem. The serial modem is always listed as "TTY Serial Port".
Location	Position of the serial port connector The serial port location always appears as "Serial Port Panel Tx/Rx (LPUART1)", which is the DB-9 serial connector on the MG90's rear panel.

Table B-4: Devices > Serial Modem screen fields (Continued)

Field	Description
Use	Select the current usage mode of the serial modem. ■ IDLE — Serial modem cannot be used for a connection at this time. ■ WAN — Serial modem can be used for a WAN connection, and will appear in the Status > WAN screen. To change the usage mode, select a different value and click Save.
Actions	Not applicable

B.5 Devices > Serial

The MG90 has a built-in DB-9 serial port on the rear panel. This port can be used by a computer to access the MG90's Linux console, or can be used to connect an external device (application) such as a serial modem or external GPS device.

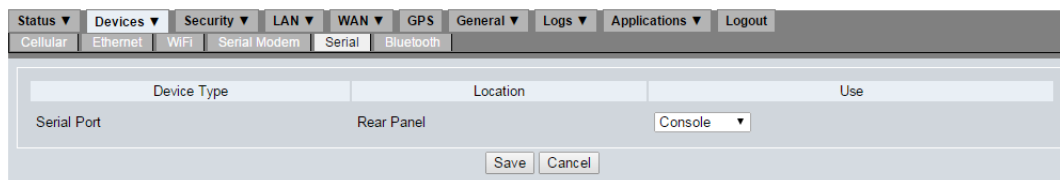


Figure B-5: LCI: Devices > Serial—Sample screen

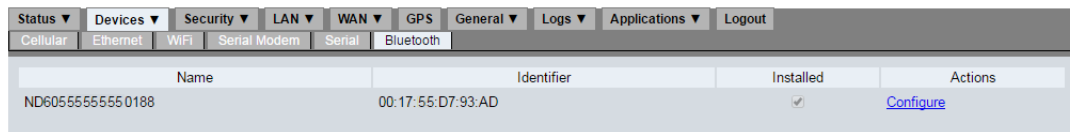
Table B-5: Devices > Serial screen fields

Field	Description
Device Type	The MG90 has a single built-in serial port (RS-232 DB9 connector) on the rear panel). The port is always listed as "Serial Port".
Location	Serial port location The location always appears as "Rear Panel".
Use	Select the current usage mode of the serial port: ■ Console — A computer will be able to connect to the MG90's Linux console. ■ Application — An external device (serial modem, GPS device, etc.) can be connected to the MG90. Additional setup is required for external devices. For example, see Devices > Serial Modem on page 129 for serial modem setup, and Setting up GPS connectivity on page 94 for external GPS device setup. To change the usage mode, select a different value and click Save. The change takes effect after you reboot the MG90 (you can press and release the Reset button on the front panel).

B.6 Devices > Bluetooth

The MG90 has an internal Bluetooth adapter for connecting multiple Bluetooth-enabled devices to the router's Bluetooth network. The internal adapter is disabled by default and must be enabled before devices can pair with it.

Note: This screen is read-only, none of the information displayed can be updated from this screen.



Name	Identifier	Installed	Actions
ND6055555550188	00:17:55:D7:93:AD	☒	Configure

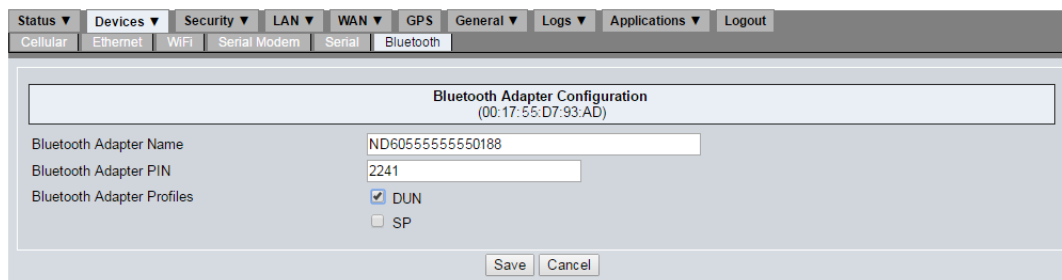
Figure B-6: LCI: Devices > Bluetooth—Sample screen

Table B-6: Devices > Bluetooth screen fields

Field	Description
Name	Descriptive name for the internal Bluetooth adapter that appears when a Bluetooth-enabled device discovers the MG90.
Identifier	Bluetooth device address code
Installed	Bluetooth adapter status - Selected — Adapter is functioning. - Not selected — Adapter is not functioning.
Actions	Configure — Click to modify the Bluetooth adapter's name, PIN, and profile. See Bluetooth Adapter Configuration (Devices > Bluetooth > Configure) on page 131.

B.6.1 Bluetooth Adapter Configuration (Devices > Bluetooth > Configure)

This screen is used to configure the internal Bluetooth adapter's descriptive name and its access options.



Bluetooth Adapter Configuration
(00:17:55:D7:93:AD)

Bluetooth Adapter Name:

Bluetooth Adapter PIN:

Bluetooth Adapter Profiles:

☒ DUN

☐ SP

Figure B-7: LCI: Devices > Bluetooth > Configure—Sample screen

Table B-7: Devices > Bluetooth > Configure screen fields

Field	Description
Bluetooth Adapter Name	Enter a descriptive name for the internal Bluetooth adapter. This name identifies the MG90 when a Bluetooth-enabled device discovers its Bluetooth adapter. For example, the name could identify the vehicle carrying the MG90, such as "Truck25".
Bluetooth Adapter PIN	Pairing code Enter the pairing code that a device needs to connect to the MG90's Bluetooth adapter. <i>Note: By default, this code is blank. A user-selected code must be entered before the screen can be saved with either Bluetooth Adapter Profile selected.</i>
Bluetooth Adapter Profiles	Bluetooth connection method Select the appropriate method that devices need to connect to the Bluetooth adapter: ▪ DUN — Device connects using a TCP/IP dial-up connection profile (e.g. ZOLL, Phillips). ▪ SP — Device connects using a serial port profile (e.g. Physio LIFEPAK 12/15). If both methods are deselected, the adapter is disabled and devices cannot pair with it. <i>Note: By default, the adapter is disabled (both profiles are deselected). If enabling either profile, a Bluetooth Adapter PIN must also be assigned before the screen can be saved.</i>

C: Security Tab

This chapter describes the Security tab, which is used to manage user and root access to the MG90.

The Security tab includes the following sub-tabs:

- Users — Add, edit (update), and delete user accounts. See [Security > Users](#) on page 133.
- Change Root Password — Change the default root access password. See [Security > Change Root Password](#) on page 134.
- Certificate Management — Create certificate profiles for existing certificates and for new certificates. See [Security > Certificate Management](#) on page 135.
- Settings — Choose the supported LCI connection protocols. See [Security > Settings](#) on page 140.

C.1 Security > Users

The Users tab is used to display and configure the names, passwords, and access methods for users that can access the LCI.

User Name	Role	Action
admin	Administrator	Edit Delete
user	User	Edit Delete

Figure C-1: LCI: Security > Users—Sample screen

Table C-1: Security > Users screen fields / buttons

Field	Description
Add / Edit User (Top half of screen)	
Login Name	Unique user name Enter a unique name for the user account that is being added / updated. Requirements: ▪ Must be POSIX-compliant: • Length: 2–28 characters • Supported characters: 'A'–'Z', 'a'–'z', '0'–'9', period ('.'), underscore ('_'), hyphen ('-')
Password	User password Enter a non-blank password for the user account. Requirements: ▪ Minimum length: 8 characters ▪ Must include at least one uppercase ('A'–'Z'), one lowercase ('a'–'z'), and one numeric ('0'–'9')
Confirm Password	Re-enter the user password to ensure it was entered correctly.

Table C-1: Security > Users screen fields / buttons (Continued)

Field	Description
Role	User type Select the access level for the user account: - User — User can access Status > WAN screen only. - Administrator — User can access all LCI screens.
Add User (button) or Edit User (button)	Button to add a new user or edit an existing user - Add User — Default button when page is displayed. Click to add a new user with the name, password, and role entered above. - Edit User — Button appears when you click the 'Edit' link for a user in the users list. Change any of the fields above, and click to save the changes.
Users List (Bottom half of screen)	
User Name	Login name of an existing user
Role	User type - User — User can access the LCI WAN Link Status screen only. - Administrator — User has full access to all LCI screens.
Action	Click these optional links to perform actions on the associated users: - Edit — Display the user details (name and role), enter a new password, and optionally change the user role. - Delete — Remove the user from the system. When prompted, click OK to confirm the deletion.

C.2 Security > Change Root Password

The Change Root Password tab is used to change the root password. When the screen appears, all fields are blank. See [Changing the Root Password](#) on page 32 for details.

Important: *If you forget the root password, it cannot be recovered. Perform a factory reset to restore it to the default value (the MG90's serial number). To perform the factory reset, press and hold the Reset button on the MG90's front panel until all the LEDs turn solid white. Release the button, and the LEDs remain white while the factory reset is in progress. The LEDs return to their normal behavior when the factory reset finishes.*

Figure C-2: LCI: Security > Change Root Password—Sample screen

Table C-2: Security > Change Root Password screen fields

Field	Description
Old root password	Enter the current root password If needed, contact Sierra Wireless Technical Support for the default password (see Contact Information on page 3).
New root password	Enter a new, non-blank password, minimum 8 characters.
Re-enter new password	Re-enter the new password to confirm.
Change (button)	Click to save the new password.

C.3 Security > Certificate Management

The Certificate Management tab is used to create certificate profiles for existing certificates and for new certificates. See [Certificate Profile Management](#) on page 85 for details.

The following figure and table describe the Certificate Profiles screen that first appears on the Certificate Management tab.

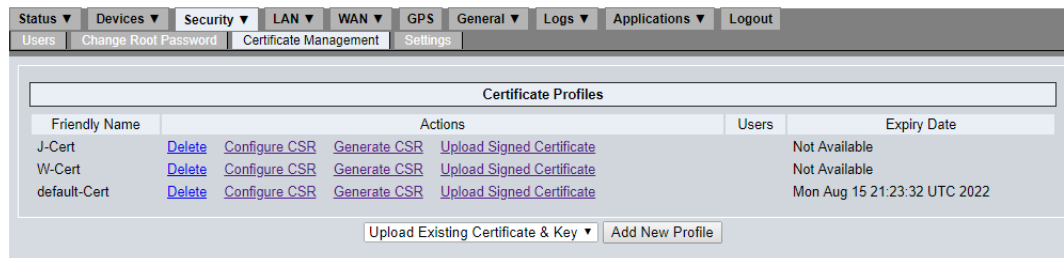


Figure C-3: LCI: Security > Certificate Management—Sample screen

Table C-3: Security > Certificate Management screen fields

Field	Description
Profile Name	Descriptive name that was assigned when the profile was added.
Actions	Click these optional links to perform actions on the associated profiles: - Delete — Delete the profile. - Configure CSR — Click to modify the profile details. After modifying the details, generate a new CSR file to obtain a new certificate from a CSA. - Generate CSR — Click to generate a CSR file that can be used to obtain a new certificate from a CSA. - Upload Signed Certificate — After obtaining a certificate for the profile from a CSA, click to upload the certificate to the router. The Users and Expiry Date fields will fill automatically.
Users	(Read-only) The VPN profile or Wi-Fi network profile that is using this certificate.
Expiry Date	(Read-only) The expiry date of the signed certificate.

C.3.1 Existing Certificate/Key Upload Screen

The following figures and table describe the screen that appears when Upload Existing Certificate & Key is selected from the Certificate Profiles screen. (LCI-initiated — Legacy method on page 88.)

This option will be used by customers who obtain signed certificates using CSRs created outside of the router.

After entering all the fields, press Save to validate the information against the selected certificate before uploading it to the router.

The screenshot shows the 'Existing Certificate/Key Upload' configuration page. The top navigation bar includes tabs for Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below this is a sub-navigation bar with Users, Change Root Password, Certificate Management, and Settings. The main content area is titled 'Existing Certificate/Key Upload' and contains the following fields:

- Profile Name: default-1
- Certificate File Type: PEM
- Client Certificate File: Choose File (No file chosen)
- Private Key File: Choose File (No file chosen)
- Private Key Password: [password field]

At the bottom right are 'Save' and 'Cancel' buttons.

Figure C-4: LCI: Security > Certificate Management > Existing Certificate/Key Upload (PEM file)

The screenshot shows the 'Existing Certificate/Key Upload' configuration page for a PFX file. The layout is similar to Figure C-4, but the 'Certificate File Type' is set to 'PFX'. The fields are:

- Profile Name: default-1
- Certificate File Type: PFX
- Client Certificate File: Choose File (No file chosen)
- PFX Import Password: [password field]

'Save' and 'Cancel' buttons are at the bottom right.

Figure C-5: LCI: Security > Certificate Management > Existing Certificate/Key Upload (PFX file)

Table C-4: Existing Certificate/Key Upload screen fields

Field	Description
Profile Name	Descriptive name to identify the profile in other screens.
Certificate File Type	Certificate format - PEM — (Privacy Enhanced Mail) Base64 encoded DER format certificate - PFX — X.509 format certificate
Client Certificate File (Button)	Click 'Choose File' button to select the certificate file to upload from your computer.
Private Key File (Button)	Click 'Choose File' button to upload the private key file that was used to obtain the PEM certificate. <i>Note: This field appears only if the Certificate File Type is PEM.</i>

Table C-4: Existing Certificate/Key Upload screen fields (Continued)

Field	Description
PFX Import Password	Enter the password provided with the PFX certificate. <i>Note: This field appears only if the Certificate File Type is PFX.</i>
Private Key Password	Enter the private key file's password. <i>Note: This field appears only if the Certificate File Type is PEM.</i>

C.3.2 CSR Configuration Screen

The following figure and table describe the screen that appears when either Configure New CSR is selected to add a new profile or Configure CSR is selected from the Certificate Profiles screen. (LCI-initiated — Secure method on page 86.)

This screen includes the X.509 attributes that are required to generate a CSR.

The screenshot shows the 'CSR Configuration' window. At the top, there's a navigation bar with tabs: Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below this is a sub-menu bar with: Users, Change Root Password, Certificate Management, and Settings. The main window has a title bar 'CSR Configuration'. Inside, the 'Profile Name' is 'J-Cert'. The 'Key Algorithm' is set to 'RSA', 'Key Size' to '2048', and 'Signature Algorithm' to 'SHA384'. The 'Distinguished Name' section includes fields for Common Name (*), Department Name, Organization Name, City, State/Province, and Country Code (2 Letters). The 'Subject Alternative Name' section includes fields for Email Address, Domain Name, IP Address, URI, and User Principal Name. At the bottom, there are 'Save' and 'Cancel' buttons.

Figure C-6: LCI: Security > Certificate Management > Configure CSR—Sample screen

Table C-5: CSR Configuration screen fields

Field	Description
Profile Name	Descriptive name to identify the profile in other screens.
Key Algorithm	Signing algorithm that was used to sign the certificate - ECDSA - RSA <i>Important: If the requested certificate will be used for a VPN:</i> - ECDSA must be selected if the MG90 is FIPS-enabled. - RSA must be selected if the MG90 is not FIPS-enabled.

Table C-5: CSR Configuration screen fields (Continued)

Field	Description
Key Size	Length of key (in bits) that was used to sign the certificate 256 — ECDSA only 384 — ECDSA only 512 — ECDSA only 1024 — RSA only 2048 — RSA only 4096 — RSA only
Signature Algorithm	Signing algorithm that was used to sign the certificate - SHA256 - SHA384 - SHA512
Distinguished Name (Fields typically used for certificate creation) <i>Note: Special characters (including < > ~ ! @ # \$ % ^ * / \ () ? . , &) are not allowed in any Distinguished name fields.</i>	
Common Name (*)	(This is a required field.) Name of certificate requester (e.g. Organization name)
Department Name	Department name within your organization
Organization Name	Organization (e.g. company) name
City	Organization's city
State/Province	Organization's state
County Code (2 Letters)	Organization's country (two-letter ISO country code. e.g. "US", "CA") For valid codes, see en.wikipedia.org/wiki/List_of_ISO_3166_country_codes .
Subject Alternative Name (Fields that may need to be used to identify requester) <i>Important: Any Subject Alternative Name fields with more than one value (e.g. two domain names) must use commas (,) to separate them. Do not use spaces as the values will merge.</i> <i>e.g. 'www1.test.com, www2.test.com' is valid; 'www1.test.com www2.test.com' will merge into 'www1.test.comwww2.test.com'</i>	
Email Address	Email address of certificate requester
Domain Name	Domain name of requester (e.g. xyzcompany.com)
IP Address	IP address of requester Valid format: IP address format (e.g. 192.168.1.2). Do not use FQDN.

Table C-5: CSR Configuration screen fields (Continued)

Field	Description
URI	Uniform Resource Identifier - Valid values: - Blank - URI 'scheme' following the generic syntax: <i>scheme:[//authority]path[?query][#fragment]</i> - For example: mailto:John.Doe@example.com https://john.doe@www.example.com:123/forum/questions/?tag=networking&order=newest#top
User Principal Name	User principal name (UPN)— email address of the requester used for LDAP authentication (user validation in an Active Directory).

C.3.3 Certificate Signing Request Summary Screen

The following figure shows the screen that appears when Generate CSR is selected from the Certificate Profiles screen. (LCI-initiated— Legacy method on page 88.)

All fields are display-only. (For definitions, see [Table C-5](#) on page 137.)

To generate a CSR that can be submitted by the user to a certificate signing authority (CSA) to obtain a new certificate:

1. Review the displayed information to make sure that it is all correct.
2. Click Generate CSR. A CSR file is stored in your browser downloads folder using the Profile Name.

Certificate Signing Request Summary

Certificate Profile Name: default

Key Algorithm (*)	RSA	Distinguished Name	
Key Size (*)	2048	Common Name (*)	JohnDoe
Signature Algorithm (*)	SHA384	Department Name	Production
		Organization Name	MyCompany
		City	Richmond
		State/Province	BC
		Country Code (2 Letters)	US

Subject Alternative Name

Email Address	jdoe@mycompany.com
Domain Name	mycompany98273.com
IP Address	205.206.163.40
URI	https://jdoe@mycompany.com:123/forum/questions/?tag=networking&order=newest#top
User Principal Name	jdoe@mycompany.com

Generate CSR Cancel

Figure C-7: LCI: Security > Certificate Management > Generate CSR—Sample screen

C.3.4 Signed Certificate Upload Screen

The following figure shows the screen that appears when Upload Signed Certificate is selected from the Certificate Profiles screen.

After generating a CSR and obtaining a signed certificate from a CSA, upload the certificate to the router:

1. Check the Profile Name to make sure the correct profile was selected for the certificate being uploaded.

2. Click Choose File and select the signed certificate to be uploaded.
3. Click Save. The certificate is validated against the CSR, and if they match (the correct certificate has been selected), the certificate's Expiry Date will appear in the Certificate Profiles list.

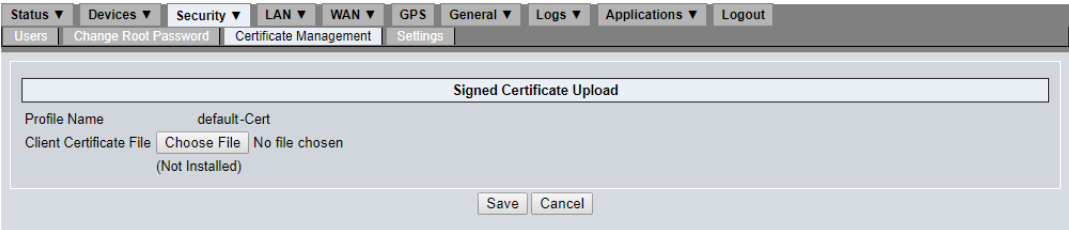


Figure C-8: LCI: Security > Certificate Management > Upload Signed Certificate—Sample screen

C.4 Security > Settings

The Settings tab is used to select the supported access protocols for the LCI — HTTPS only, or HTTP + HTTPS).

See [Configuring Supported LCI Access Protocols](#) on page 32 for usage details.

The following figure and table describe the Settings tab.

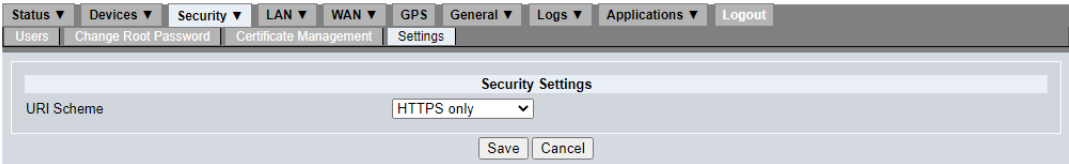


Figure C-9: LCI: Security > Settings—Sample screen

Table C-6: Security > Settings screen fields

Field	Description
URI Scheme	Uniform Resource Identifier—Supported LCI access protocols ▪ HTTPS only—(Default) LCI can only be accessed using https. ▪ HTTP and HTTPS—Both methods are supported. <i>Note: If the URI scheme is changed from 'HTTPS only' to 'HTTP and HTTPS', you must clear the browser cache before attempting to log in using HTTP.</i>

D: LAN Tab

This chapter describes the LAN tab, which is used to manage the MG90's LAN.

The LAN tab includes the following sub-tabs:

- Ethernet Links — Configure the MG90's Ethernet ports for LAN use. See [LAN > Ethernet Links](#) on page 141.
- Access Points — Configure the MG90's Wi-Fi radios as access points for devices to connect to the MG90's LAN. See [LAN > Access Points](#) on page 144.
- LAN Segments — Configure the LAN as one or more segments for advanced networking scenarios. See [LAN > LAN Segments](#) on page 153.
- Virtual LANs — Configure virtual LANs for security purposes, VLAN tagging, etc. See [VLAN Configuration \(LAN > Virtual LANs\)](#) on page 156.
- Networking Rules — Configure rules to block or permit specific devices on the LAN, and to ensure quality of service. See [LAN > Networking Rules](#), and [LAN > LAN Segments > Networking Rules](#) on page 158.
- LAN Throughput — Configure LAN throughput reporting. See [LAN > LAN Throughput](#) on page 163.
- Captive Portal — Configure captive portals for Wi-Fi access points. See [LAN > Captive Portal](#) on page 164.

D.1 LAN > Ethernet Links

This screen lists the Ethernet ports ('links') that are currently selected for LAN in Devices > Ethernet, and the available Actions for configuring them.

For example, [Figure D-1](#) does not show "Panel Ethernet 1" because that port is currently configured for WAN use.

Device Type	Friendly Name	Configure
Device Built-in Ethernet Port	Panel Ethernet 1	Configure
Device Built-in Ethernet Port	Panel Ethernet 2	Configure
Device Built-in Ethernet Port	Panel Ethernet 3	Configure
Device Built-in Ethernet Port	Panel Ethernet 4	Configure

Figure D-1: LCI: LAN > Ethernet Links—Sample screen

Table D-1: LAN > Ethernet Links screen fields

Field	Description
Device Type	Hardware device type (cannot be modified). Always appears as "Device Built-in Ethernet Port"
Friendly Name	Friendly name defined in Devices > Ethernet
Configure	Click to configure the LAN connection options. See LAN Ethernet Configuration (LAN > Ethernet Links > Configure) on page 141.

D.1.1 LAN Ethernet Configuration (LAN > Ethernet Links > Configure)

This screen is used to enable (or disable) and configure 802.1x network access control for a LAN-enabled Ethernet port.

Figure D-2: LCI: LAN > Ethernet Links > Configure—Sample screen

Table D-2: LAN > Ethernet Links > Configure screen fields

Field	Description
Enable wired 802.1x network access control	802.1x network access control state - Selected— Enable 802.1x network access control and display the configuration fields. - Not selected — Disable network access control. Any device physically connected to the port can access the network. <i>Note: If this is enabled, at least one Authentication server must be entered and enabled.</i>
802.1x Options (These fields appear only if Enable wired 802.1x network access control is selected.)	
Primary 802.1x Retry Interval (secs)	Number of seconds the system waits after the primary authentication server has failed over to the secondary server before trying to reconnect to the primary server. Default: 300 (5 minutes) <i>Note: The system sends to the secondary only if the primary fails.</i>
Interim 802.1x Accounting Interval (secs, 0 to disable)	Number of seconds that the system waits between submissions of interim accounting data. 0—Disable 1 or higher —Wait this number of seconds between submissions - Default: 300 (5 minutes) <i>Note: Data transmits automatically when a login session starts and stops.</i>

Table D-2: LAN > Ethernet Links > Configure screen fields (Continued)

Field	Description
Enable EAP Re-authentication Period	Select to force system to periodically renegotiate connection credentials. - Selected — System automatically re-authenticates (renegotiates connection credentials) after the EAP Re-authentication Period. - Not selected — Full re-keying is required each time the MG90 moves into an area served by a different authenticator.
EAP Re-authentication Period (secs)	Number of seconds between authentications (if Enable EAP Re-authentication Period is selected) Default: 3600 (60 minutes) <i>Note: Use a long re-authentication period (e.g. the default period — 3600 seconds) to delay the need to re-authenticate when a WAN connection is interrupted.</i>
Enable Cisco Legacy 802.1x Compatibility	Select to enable for systems that use lower case MAC addresses in the calling station ID field. This is recommended for interoperability with the Cisco RADIUS implementation.
802.1x Authentication Servers (These fields appear only if Enable wired 802.1x network access control is selected.)	
<i>Note: At least one authentication server must be enabled.</i>	
<i>Warning: If a user logs out of their Windows system after authenticating with the 802.1x server, another Windows user can log in and access the network without re-authenticating. This is driven by the Windows system.</i>	
Primary (To access these fields, select Enabled.)	
Address	IP address or host name of the primary RADIUS authentication server
Port	Port number used to access the authentication server
Secret	Shared secret code required to access the authentication server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
Enabled	Select to enable access to the primary authentication server.
Secondary (To access these fields, select Enabled.)	
Address	IP address or host name of the secondary RADIUS authentication server
Port	Port number used to access the authentication server
Secret	Shared secret code required to access the authentication server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
Enabled	Select to enable access to the secondary authentication server. <i>Note: The secondary server is used only if the primary is not enabled, or the primary fails.</i>
802.1x Accounting Servers (These fields appear only if Enable wired 802.1x network access control is selected.)	
<i>Note: Accounting servers are optional.</i>	
Primary (To access these fields, select Enabled.)	
Address	IP address or host name of the primary RADIUS accounting server
Port	Port number used to access the accounting server

Table D-2: LAN > Ethernet Links > Configure screen fields (Continued)

Field	Description
Secret	Shared secret code required to access the accounting server from the MG90. If the shared secret is incorrect, the server ignores accounting requests.
Enabled	Select to enable access to the primary accounting server
Secondary (To access these fields, select Enabled.)	
Address	IP address or host name of the secondary RADIUS accounting server
Port	Port number used to access the accounting server
Secret	Shared secret code required to access the accounting server from the MG90. If the shared secret is incorrect, the server ignores accounting requests.
Enabled	Select to enable access to the secondary authentication server. <i>Note: The secondary server is used only if the primary is not enabled, or the primary fails.</i>

D.2 LAN > Access Points

The Access Points tab lists all devices that can be configured as Wi-Fi access points.

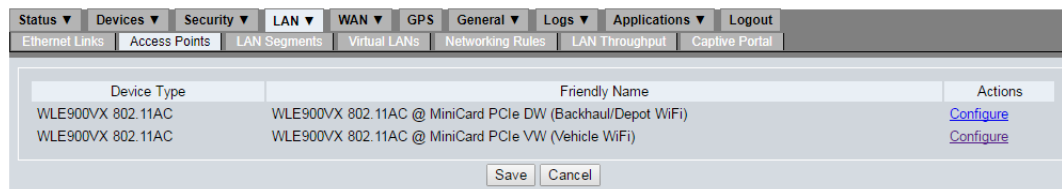


Figure D-3: LCI: LAN > Access Points—Sample screen

Table D-3: LAN > Access Points screen fields

Field	Description
Device Type	Device type identification The device type shown is a combination of the Wi-Fi module type and the network access control type (802.1x) used by the AP.
Friendly Name	Descriptive name for the Wi-Fi device. To change the description, see Devices > Wi-Fi on page 128.
Actions	Click these optional links to perform actions on the associated access points: Configure — Click to configure the device as an access point. See Access Point Configuration (LAN > Access Points > Configure) on page 144.

D.2.1 Access Point Configuration (LAN > Access Points > Configure)

This screen is used to configure a Wi-Fi device as an access point.

Note: The screen details depend on the Network Type and Encryption values. [Figure D-4](#) shows one combination.

Access Point Configuration
(WLE900VX 802.11AC @ MiniCard PCIe WiFi B)

802.11 Configuration

Enabled ☒

Network Type 802.11ac ▾

Auto SSID ☒

SSID ND88888888888888

Broadcast SSID ☒

Captive Portal ☒ Conference Center Premium ☐ Hotel Portal

Channel (Frequency in MHz) 36 (5180) ▾

Secondary Channel above ▾

Enable Multiple Antennas (802.11 n/ac MIMO) ☐

Channel Width (802.11 ac) 80 ▾

Enable WMM ☒

Enable AP Isolation ☒

MAC Access Control List DISABLED ▾

Encryption None ▾

Virtual BSSIDs

Virtual BSSID 1 Enable ☒ Show/Hide

Auto SSID ☒ SSID ND88888888888888_1

Broadcast SSID ☒

Captive Portal ☐ Conference Center Premium ☐ Hotel Portal

Enable WMM ☒

Enable AP Isolation ☒

MAC Access Control List DISABLED ▾

Encryption None ▾

Virtual BSSID 2 Enable ☐ Show/Hide

Virtual BSSID 3 Enable ☐ Show/Hide

Figure D-4: LCI: LAN > Access Points > Configure—Sample screen

Table D-4: LAN > Access Points > Configure screen fields

Field	Description
802.11 Configuration	
Enabled	Access Point state - Selected — Enabled - Not selected — (Default) Disabled <i>Note: Disabling the Access Point does not affect any configuration settings, it only prevents the Access Point from being used.</i>
Network Type	802.11 network access control protocol used by the access point 802.11a/b/g 802.11n 802.11ac (Default)
Auto SSID	Automatically generate the primary SSID (Basic Service Set Identifier) and virtual SSIDs - Selected — The MG90's serial number is used for the primary SSID, and the serial number followed by an underscore and a digit (i.e. <ESN>_1) is used for virtual SSIDs (BSSID 1, BSSID 2, BSSID 3). - Not selected — SSID field is set manually.

Table D-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
SSID	Basic Service Set Identifier This identifier appears when a device scans for access points and detects the MG90. Default value: MG90's serial number <i>Note: This field is accessible only if Auto SSID is not selected.</i>
Broadcast SSID	Broadcast the SSID - Selected (Default) — Devices will see the SSID when scanning for access points. - Not selected — SSID is not visible to devices scanning for access points.
Captive Portal	Captive portal that users must connect through when using the access point. Only one portal can be selected at any time. - No portal selected — Access point is not restricted by a captive portal - Portal selected — Wi-Fi access is controlled by the captive portal as defined in LAN > Captive Portal > Configure on page 165. "not defined" — No portals are defined in LAN > Captive Portal > Configure on page 165. <i>Note: Captive Portal support requires that only one Wi-Fi module is configured as an access point.</i>
Channel (Frequency in MHz)	Wi-Fi channel/frequency (i.e. the center frequency) within the spectrum to be used The list of available channels varies depending on the selected Network Type. <i>Note: When choosing the channel, consider other devices that may interfere with the channel (including other Wi-Fi devices in the MG90).</i>
Secondary Channel	Secondary channel position for increased bandwidth A secondary channel is combined with the primary channel to provide a 40 MHz channel (for 802.11n) or 80 MHz channel (for 802.11ac) instead of 20 MHz or 40 MHz, respectively. The available options depend on the primary channel. For some primary channels, the secondary channel can only be below the primary; for others, it can only be above; for others it can be either. If set, the secondary channel's position will be relative to (i.e. below or above) the primary channel in the spectrum. Options: - none - above - below <i>Note: This field is not available when the Network Type is 802.11a/b/g.</i>
Enable Multiple Antennas (802.11n/ac MIMO)	MIMO (multiple antennas) support for 802.11n or 802.11ac. - Selected — MIMO is supported - Not selected — MIMO is not supported
Channel Width (802.11 ac)	Bandwidth for 802.11ac 20 MHz 40 MHz (Default) 80 MHz
Enable WMM	WMM (Wireless MultiMedia extensions) support Make sure that this value is always selected.

Table D-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
Enable AP Isolation	Access Point Isolation - Selected — Clients on the access point cannot access each other. - Not selected — Clients on the access point can access each other.
MAC Access Control List	Enable or disable MAC access control (whitelist or blacklist) of devices attempting to connect to the access point. (Also known as 'MAC filtering.') - DISABLED (default) — Disable MAC address filtering. - ACCEPT — "Whitelist" mode. Only devices with MAC addresses in the whitelist file (described below) can connect to the access point. - DENY — "Blacklist" mode. Devices with MAC addresses in the blacklist file (described below) are not allowed to connect to the access point. The whitelist and blacklist files should be created as described below, and issued to devices via AMM. File requirements: - Whitelist location: /opt/inmotiontechnology/config/global.accept.txt - Blacklist location: /opt/inmotiontechnology/config/global.deny.txt - Plain ASCII text - Comment lines may be used and will start with the octothorpe ('#') character - Blank lines are permitted - MAC addresses: - One address per line - Format: hh:hh:hh:hh:hh:hh (Six hexadecimal digit pairs) - Lines with malformed addresses are ignored. When a malformed address is encountered, it is logged in /opt/inmotiontechnology/logs/YYYY-MM-DDlan.log. Example (blacklist shown, whitelist uses identical format): <pre># List of MAC addresses that are not allowed to authenticate (IEEE 802.11) with the AP. 00:20:30:40:50:60 00:ab:cd:ef:12:34 00:00:30:40:50:60</pre>
Encryption	Encryption type used by the access point Depending on the encryption type, various configuration fields will appear. - None — Access point is unsecured. - WEP — Secure access via WEP - WPA/TKIP — Secure access via WPA/TKIP - WPA2/CCMP — Secure access via WPA2/CCMP <i>Note: None and WPA2/CCMP are the only options if Network Type is 802.11n or 802.11ac.</i>
WEP-specific configuration fields (These fields appear only if Encryption type is "WEP".)	
WEP Key Length	WEP Key length 40-bit 104-bit
Change WEP Key	Select to access the next three fields. <i>Note: This field appears only if you are updating an existing AP configuration that has WEP encryption.</i>

Table D-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
Previous WEP Key	The current WEP key being used. <i>Note: This field appears only if you are updating an existing AP configuration that has WEP encryption.</i>
WEP Key or New WEP Key	WEP security key Enter the key that devices must use to connect to the access point. - Hexadecimal characters only ('0'–'9','a'–'f','A'–'F') - Fill in all 'white' blocks (each block is 8 bits (two hexadecimal characters))
Retype WEP Key or Retype New WEP Key	Re-enter the WEP key to ensure it was entered correctly.
WEP Re-key Interval (sec)	Specifies how often (in seconds) to re-negotiate the keys to be used for WEP security
WPA2 (/TKIP and /CCMP)-specific configuration fields (These fields appear only if Encryption type is "WPA2/TKIP" or "WPA2/CCMP".)	
WPA Key Management	Key management protocol - WPA-PSK — Devices use a pre-shared key for authentication. - WPA-EAP — Devices are authenticated by a RADIUS authentication server.
Change WPA Key	Select to access the next three fields. <i>Note: This field appears only if you are updating an existing AP configuration that has WPA Key Management type WPA-PSK.</i>
Previous WPA Pre-Shared Key	The current WPA pre-shared key being used. <i>Note: This field appears only if you are updating an existing AP configuration that has WPA Key Management type WPA-PSK.</i>
WPA Pre-Shared Key or New WPA Pre-Shared Key	Pre-shared key that devices must use to authenticate to the access point. Format: 8-63 ASCII characters - or 64 hexadecimal characters <i>Note: This field appears only if WPA Key Management type is WPA-PSK.</i>
Retype WPA Pre-Shared Key or Retype New WPA Pre-Shared Key	Re-enter the WPA pre-shared key to ensure it was entered correctly. <i>Note: This field appears only if WPA Key Management type is WPA-PSK.</i>
WPA GTK Rekey Interval (secs)	Specifies how often (in seconds) to renegotiate the Group Temporal Key - Default: 300 - Valid range: 1–99999 <i>Note: This field appears only if WPA Key Management type is WPA-PSK.</i>

Table D-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
WPA GMK Rekey Interval (secs)	Specifies how often (in seconds) to renegotiate the Group Master Key. - Default: 86400 - Valid range: 1–99999 <i>Note: This field appears only if WPA Key Management type is WPA-PSK.</i>
Enable 802.1x	Select to enable 802.1x network access control and display the configuration fields. <i>Note: This field appears only if WPA Key Management type is WPA-EAP.</i>
Enable Cisco Legacy 802.1x Compatibility	Select to enable for systems that use lower case MAC addresses in the calling station ID field. This is recommended for interoperability with the Cisco RADIUS implementation. <i>Note: This field appears only if Enable 802.1x is selected.</i>
Primary 802.1x Retry Interval (secs)	Number of seconds the system waits after the primary authentication server has failed over to the secondary server before trying to reconnect to the primary server. Default: 300 (5 minutes) <i>Note: The system sends to the secondary only if the primary fails.</i> <i>Note: This field appears only if Enable 802.1x is selected.</i>
Interim 802.1x Accounting Interval (secs, 0 to disable)	Number of seconds that the system waits between submissions of interim accounting data. 0 — Disable 1 or higher — Wait this number of seconds between submissions - Default: 300 (5 minutes) <i>Note: Data transmits automatically when a login session starts and stops.</i> <i>Note: This field appears only if Enable 802.1x is selected.</i>
Enable EAP Re-authentication Period	Select to force system to periodically renegotiate connection credentials. - Selected — System automatically re-authenticates (renegotiates connection credentials) after the EAP Re-authentication Period. - Not selected — Full re-keying is required each time the MG90 moves into the area served by a different authenticator.) <i>Note: This field appears only if Enable 802.1x is selected.</i>
EAP Re-authentication Period (secs)	Number of seconds between authentications (if Enable EAP Re-authentication Period is selected) Default: 3600 (60 minutes) <i>Note: Use a long re-authentication period (e.g. the default period — 3600 seconds) to delay the need to re-authenticate when a WAN connection is interrupted.</i> <i>Note: This field appears only if Enable 802.1x is selected.</i>
802.1x Authentication Servers (These fields only appear if Enable 802.1x is selected.)	
<i>Note: At least one authentication server must be enabled.</i>	
Primary (To access these fields, select Enabled.)	
Address	IP address or host name of the primary RADIUS authentication server.
Port	Port number used to access the authentication server.

Table D-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
Secret	Shared secret code required to access the authentication server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
Enabled	Select to enable access to the primary authentication server.
Secondary (To access these fields, select Enabled.)	
Address	IP address or host name of the secondary RADIUS authentication server.
Port	Port number used to access the authentication server.
Secret	Shared secret code required to access the authentication server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
Enabled	Select to enable access to the secondary authentication server. <i>Note: The secondary server is used only if the primary is not enabled, or the primary fails.</i>
802.1x Accounting Servers (These fields only appear if Enable 802.1x is selected.)	
<i>Note: Accounting servers are optional.</i>	
Primary (To access these fields, select Enabled.)	
Address	IP address or host name of the primary RADIUS accounting server.
Port	Port number used to access the accounting server.
Secret	Shared secret code required to access the accounting server from the MG90. If the shared secret is incorrect, the server ignores accounting requests.
Enabled	Select to enable access to the primary accounting server.
Secondary (To access these fields, select Enabled.)	
Address	IP address or host name of the secondary RADIUS accounting server.
Port	Port number used to access the accounting server.
Secret	Shared secret code required to access the accounting server from the MG90. If the shared secret is incorrect, the server ignores accounting requests.
Enabled	Select to enable access to the secondary authentication server. <i>Note: The secondary server is used only if the primary is not enabled, or the primary fails.</i>
Virtual BSSIDs	
Up to three virtual BSSIDs (Basic SSIDs) can be configured for a particular access point (AP). This means that the AP can appear to clients as up to four different APs, each with its own SSID and security configuration.	
Virtual BSSID 1	
Enable	Select to make this virtual BSSID available, using the configuration settings below.
Show/Hide (button)	Click to show /hide the configuration Virtual BSSID's configuration fields.

Table D-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
Auto SSID	Automatically generate the SSID: - Selected — Set the SSID to the primary SSID followed by an underscore and a digit (e.g. <primarySSID>_1 is used for Virtual BSSID 1). - Not selected — SSID field is set manually.
SSID	Basic Service Set Identifier The identifier that appears to a device when it scans for access points. <i>Note: This field is accessible only if Auto SSID is not selected.</i>
Broadcast SSID	Broadcast the SSID - Selected — Devices will see the SSID when scanning for access points. - Not selected — SSID is not visible to devices scanning for access points. - Default: Selected
Captive Portal	Captive portal that users must connect through when using the access point. Only one portal can be selected at any time. - No portal selected — Access point is not restricted by a captive portal - Portal selected — Wi-Fi access is controlled by the captive portal as defined in LAN > Captive Portal > Configure on page 165. "not defined" — No portals are defined in LAN > Captive Portal > Configure on page 165. <i>Note: Captive Portal support requires that only one Wi-Fi module is configured as an access point.</i>
Enable WMM	WMM (Wireless MultiMedia extensions) support Make sure that this value is always selected.
Enable AP Isolation	Access Point Isolation - Selected — Clients on the access point cannot access each other. - Not selected — Clients on the access point can access each other.

Table D-4: LAN > Access Points > Configure screen fields (Continued)

Field	Description
MAC Access Control List	Enable or disable MAC access control (whitelist or blacklist) of devices attempting to connect to the access point. (Also known as 'MAC filtering.') - DISABLED (default) — Disable MAC address filtering. - ACCEPT — "Whitelist" mode. Only devices whose MAC addresses are in the whitelist file (described below) can connect to the access point. - DENY — "Blacklist" mode. Devices whose MAC addresses are in the blacklist file (described below) are not allowed to connect to the access point. The whitelist and blacklist files should be created as described below, and issued to devices via AMM. File requirements: - Whitelist location: /opt/inmotiontechnology/config/global.accept.txt Blacklist location: /opt/inmotiontechnology/config/global.deny.txt - Plain ASCII text - Comment lines may be used and will start with the octothorpe (#) character - Blank lines are permitted - MAC addresses: - One address per line - Format: hh:hh:hh:hh:hh:hh (Six pairs of hexadecimal digits) - Lines with malformed addresses are ignored. When a malformed address is encountered, it is logged in /opt/inmotiontechnology/logs/YYYY-MM-DDlan.log. Example (blacklist shown, whitelist uses identical format): <pre># List of MAC addresses that are not allowed to authenticate (IEEE 802.11) with the AP. 00:20:30:40:50:60 00:ab:cd:ef:12:34 00:00:30:40:50:60</pre>
Encryption	Encryption type used by the access point Depending on the encryption type, various configuration fields will appear. - None — Access point is unsecured. - WEP — Secure access via WEP - WPA/TKIP — Secure access via WPA/TKIP - WPA2/CCMP — Secure access via WPA2/CCMP
Virtual BSSID 2	Same fields as Virtual BSSID 1
Virtual BSSID 3	Same fields as Virtual BSSID 2

D.3 LAN > LAN Segments

This screen is used to assign LAN-capable devices to LAN segments.

For details on LAN segmentation, see [Configuring LAN Segments](#) on page 65.

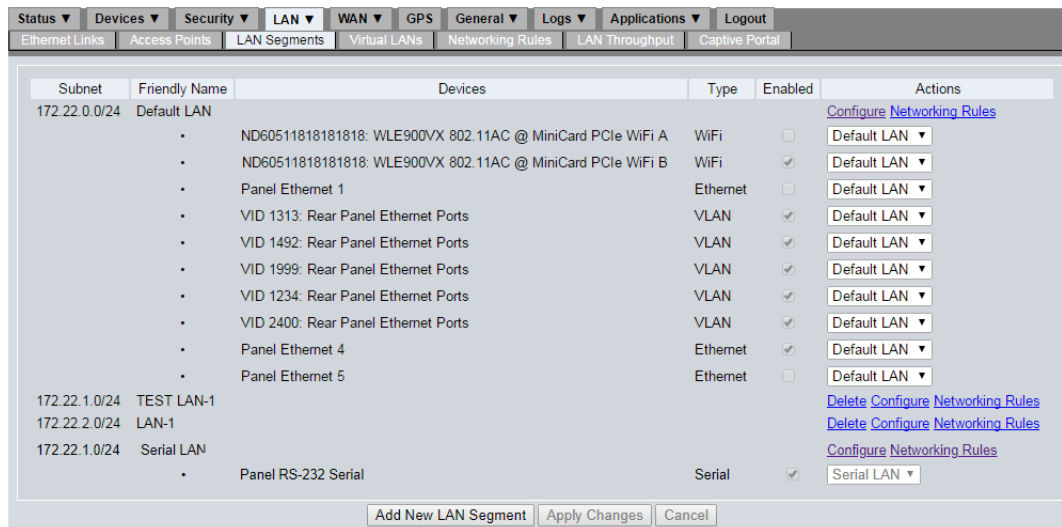


Figure D-5: LCI: LAN > LAN Segments—Sample screen

Table D-5: LAN > LAN Segments screen fields / buttons

Field	Description
Subnet	LAN segment address subnet
Friendly Name	Descriptive name for the LAN segment.
Devices	Descriptive names of devices that are associated with each LAN segment - Wi-Fi devices— Combination of the device's SSID and Friendly Name. - Ethernet devices— The device's Friendly Name. - Virtual LANs — VID number.
Type	Device type - Ethernet— Pre-installed Ethernet port - VLAN — Virtual LAN on an Ethernet port - Wi-Fi — Wi-Fi radio
Enabled	Device enabled state - Selected — The device is currently enabled for LAN usage. - Not selected — The device is not currently enabled for LAN usage, or is not currently installed in the MG90. To enable the device for LAN use, see Devices > Cellular on page 126, Devices > Ethernet on page 127, or VLAN Configuration (LAN > Virtual LANs) on page 156.

Table D-5: LAN > LAN Segments screen fields / buttons (Continued)

Field	Description
Actions	Click these optional links to perform actions on the associated LAN segments: - Delete — Delete the associated LAN segment. (This option is not available for the default LAN segment.) - Configure — Configure the associated LAN segment. See LAN Segment Configuration (LAN > LAN Segments > Configure) on page 154 for details. - Networking Rules — Create networking rules (access granting, access blocking, QoS prioritizing) for the associated LAN segment. See LAN > Networking Rules, and LAN > LAN Segments > Networking Rules on page 158 for details. - Pull downs for devices — When the screen displays, all devices will show their associated LAN segment in the pull-down. To move a device from one segment to another: - Select the desired segment from the pull-down. - Click Apply Changes. <i>Note: Each device that can be enabled on a LAN segment is linked to a specific segment. If you delete a segment, the devices that were associated with it switch automatically to the Default LAN segment.</i>

D.3.1 LAN Segment Configuration (LAN > LAN Segments > Configure)

This screen is used to configure a LAN segment.

Note: The screen details depend on the LAN segment type (standard, or Serial LAN).

The screenshot displays the 'LAN Segment Configuration (Default LAN)' window. At the top, there is a navigation bar with tabs: Status, Devices, Security, LAN (selected), WAN, GPS, General, Logs, Applications, and Logout. Below this is a sub-navigation bar with tabs: Ethernet Links, Access Points, LAN Segments (selected), Virtual LANs, Networking Rules, LAN Throughput, and Captive Portal. The main configuration area includes the following fields and options:

- Friendly Name: Default LAN
- Default Gateway Address: 172.22.0.1
- Network Mask: 255.255.255.0
- Enable DHCP Server: ☒
- DHCP Low Address: 172.22.0.100
- DHCP High Address: 172.22.0.200
- DHCP Client Lease Time (sec): 28800
- Domain search list (comma-separated):
- WINS Servers (comma-separated IP addresses):
- Enable Web Portal: ☐
- Enable Subnet Management Access: ☒
- Enable Subnet SSH Shell Access: ☐
- Isolated: ☐
- IGMP Snooping: ☐
- IPv6 Addressing: None

Figure D-6: LCI: LAN > LAN Segments > Configure (Standard)—Sample screen

Figure D-7: LCI: LAN > LAN Segments > Configure (Serial LAN)—Sample screen

Table D-6: LAN > LAN Segments > Configure (Standard) screen fields

Field	Description
Friendly Name	Enter a descriptive name for the LAN segment. This name identifies the segment in other LCI screens.
Default Gateway Address	IP address of the LAN bridge
Network Mask	Network mask of the LAN bridge Recommendation: Limit this network to a class C or smaller network. (e.g. "255.255.255.0" is the netmask for a class C (/24) network).
Enable DHCP Server	DHCP Server state - Selected — DHCP enabled - Not selected — DHCP disabled.
DHCP Low Address	Enter the starting IP address of the address pool used for DHCP.
DHCP High Address	Enter the ending IP address of the address pool used for DHCP.
DHCP Client Lease Time (sec)	Number of seconds that the IP address assigned from the address pool will be valid for the client
Domain search list (comma-separated)	List of domain name servers (DNS) to be used by the client - One or more DNS server addresses, comma-separated - IPv4 address format (e.g. xxx.xxx.xxx.xxx) or FQDN
WINS Servers (comma-separated IP addresses)	List of Windows Internet Name Service (WINS) servers to be used by the client - One or more WINS server addresses, separated by commas - IPv4 address format (e.g. xxx.xxx.xxx.xxx) or FQDN
Enable Web Portal	Web portal state If the web portal feature is enabled, the MG90 can be used as a web port for clients accessing the Internet. When a client accesses the MG90's Wi-Fi network, the client must use a browser to view and agree to terms and conditions on a splash page before continuing. - Selected — Enabled. Clients will see the web portal splash page - Not selected — Disabled. Clients can access the Wi-Fi network without going through the portal. The web portal UI consists of customizable HTML and image files. Some configuration options are available in Applications > Web Portal.

Table D-6: LAN > LAN Segments > Configure (Standard) screen fields (Continued)

Field	Description
Enable Subnet Management Access	Subnet Management state - Selected — MG90 management functions (e.g. LCI, SSH, command line) can be blocked, while allowing clients to access required resources (e.g. DNS, proxy) - Not selected — MG90 management functions cannot be blocked.
Enable Subnet SSH Shell Access	Subnet shell access via SSH state - Selected — ssh access is allowed (enabled) - Not selected — ssh access is not allowed (disabled)
Isolated	LAN segment isolation - Selected — Segment is isolated (other segments cannot see it, but the isolated segment can still see other segments) - Not selected — Segment is not isolated (can be seen by other segments)
IGMP Snooping	Enable/disable IGMP (Internet Group Management Protocol) snooping - Not selected — (Default) IGMP snooping disabled. - Selected — IGMP snooping enabled.
IPv6 Addressing	IPv6 Address support - None — IPv6 addresses not used - Unique Local Addressing — IPv6 equivalent of IPv4 private addresses. Address is unique and routable within a site, but is not globally routable. - WAN Prefix Pass through — Globally routable IPv6 address that uses the carrier prefix and appends the MAC address interface. <i>Note: If Enable IPV6 is not selected in WAN > Links > Configure (Cellular), then this option is ignored.</i>

Table 4-7: LAN > LAN Segments > Configure (Serial LAN) screen fields

Field	Description
Friendly Name	(Read-only) Descriptive name for the LAN segment. This segment is always named "Serial LAN".
Default Gateway Address	IP address assigned to the MG90's serial interface Default: 172.22.1.1
Peer Address	IP address assigned to the client (e.g. Sierra Wireless GenX series device) connected to the serial interface Must be in range Default Gateway Address's subnet (e.g. if Default is 172.22.1.1, Peer Address must be 172.22.1.[2..254])

D.4 VLAN Configuration (LAN > Virtual LANs)

In the Virtual LANs tab, you can configure and enable Ethernet ports for use as Virtual LANs.

Virtual LANs (VLAN) can be used when devices inside the vehicle require VLAN tagging for their operation, or when the vehicle LAN has a switch with VLAN tagging enabled. If a vehicle has VLANs configured, or requires additional Ethernet ports, they can be added by using a switch and VLAN tagging.

VLAN Configuration

Panel Ethernet 1
 Enabled: ☐ Save
 Type: Device Built-in Ethernet Port
 Assigned VIDs: Add VID Remove VID

Panel Ethernet 2
 Enabled: ☒
 Type: Device Built-in Ethernet Port
 Assigned VIDs: 1313, 1492, 1999
 Add VID 1313 Remove VID

Panel Ethernet 3
 Enabled: ☒
 Type: Device Built-in Ethernet Port
 Assigned VIDs: 1234, 1492, 2400
 Add VID 1234 Remove VID

Panel Ethernet 4
 Enabled: ☐ Save
 Type: Device Built-in Ethernet Port
 Assigned VIDs: Add VID Remove VID

Panel Ethernet 5
 Enabled: ☐ Save

Figure D-8: LCI: LAN > Virtual LANS—Sample screen

Table D-8: LAN > Virtual LANs screen fields

Field	Description
Panel Ethernet 1	
Enabled	Select to use the device as a virtual LAN. - Selected — Device is used as a virtual LAN. - Not selected — Device is not used as a virtual LAN. <i>Note: To add or remove VIDs, select Enabled to make the Add VID and Remove VID buttons available.</i>
Type	Device type
Assigned VIDs	List of VIDs currently assigned to the VLAN
Add VID (button)	Enter a new VID and click to add it to the associated VLAN. Valid range: 2–4094
Remove VID (button)	Enter one of the Assigned VIDs to remove and click to remove it from the associated VLAN.
Panel Ethernet 2 (Same options as Panel Ethernet 1)	
Panel Ethernet 3 (Same options as Panel Ethernet 1)	
Panel Ethernet 4 (Same options as Panel Ethernet 1)	
Panel Ethernet 5 (Same options as Panel Ethernet 1)	

D.5 LAN > Networking Rules, and LAN > LAN Segments > Networking Rules

The LAN Networking Rules tab is used to define ‘global’ networking rules that apply to all LAN connections, and ‘segment’ networking rules that apply only to connections on specific LAN segments. These rules include:

- Access Blocking
- Access Granting
- QoS Prioritizing

Note: There are three ‘levels’ of networking rules — LAN segment, WAN link, and Global (LAN). If there is a conflict between any of these rules, LAN segment rules override WAN link and global rules, and WAN link rules override global rules.

The LAN Networking Rules and WAN Networking Rules use similar setup parameters. For WAN networking rules, see [WAN > Networking Rules](#) on page 220.

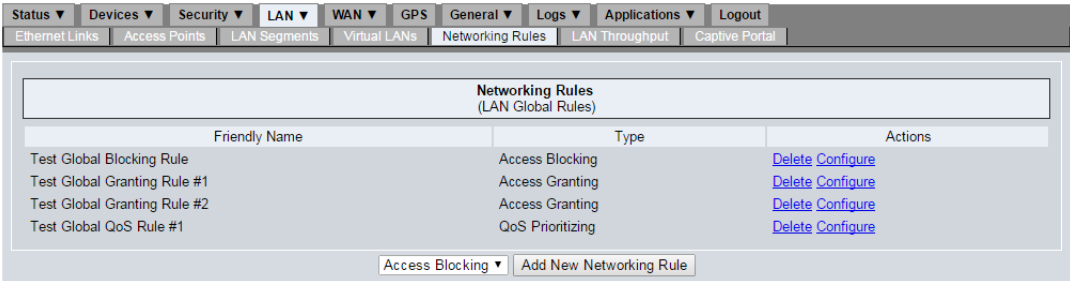


Figure D-9: LCI: LAN > Networking Rules— Sample screen

Table D-9: LAN > Networking Rules screen fields

Field	Description
Friendly Name	Descriptive name for the networking rule
Type	Rule type: ▪ Access Blocking — Block incoming or outgoing traffic. See Access Blocking Rules on page 158. ▪ Access Granting — Permit incoming or outgoing traffic. See Access Granting Rules on page 160. ▪ QoS Prioritizing — Assign traffic priority. See QoS Priority Rules on page 161.
Actions	Click these optional links to perform actions on the associated rules: ▪ Delete — Delete the associated networking rule. (This option is not available for the default LAN segment.) ▪ Configure — Configure the associated networking rule.
Add New Networking Rule	From the drop-down, select the type of rule to add to the LAN segment, and click Add New Networking Rule. For usage details, see Setting up the LAN Firewall on page 69.

Access Blocking Rules

Add an Access Blocking rule to block incoming or outgoing traffic (from the MG90's perspective) for a specific IP address, based on the criteria in [Table D-10](#) on page 159.

Tip: Fields that are left blank are treated as “wildcards”. Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.

The screenshot shows the 'Access Blocking Firewall Rule' configuration window. The title bar indicates it's for 'LAN Global Rules'. The 'Rule Name' field contains 'Test Global Blocking Rule'. The 'Direction' is set to 'Incoming'. The 'Source IP Address' is '192.168.44.27'. The 'Source Port Range' is '55' to '74'. The 'Protocol' is 'TCP'. The 'Destination IP Address' is '192.168.55.184'. The 'Destination Port Range' is '60' to '79'. The 'Action' is 'Reject'. The 'Reject Cause' is 'Unreachable'. There are 'Save' and 'Cancel' buttons at the bottom.

Figure D-10: LCI: LAN > Networking Rules > Add Rule (Access Blocking)—Sample screen

Table D-10: LAN > Networking Rules > Add Rule (Access Blocking) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule
Direction	Traffic direction relative to the MG90 - Incoming — The Source IP Address will be blocked. - Outgoing — The Destination IP Address will be blocked.
Source IP Address	Source IP address - Format: xxx.xxx.xxx.xxx[/xx] - Examples: - Address without netmask — 192.168.4.17. Applies to the stated IP address. - Address with netmask — 192.168.4.0/24. Applies to the IP address range 192.168.4.0–192.168.4.255.
Source Port Range	Starting and ending source port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port
Protocol	Communications protocol - TCP - UDP - TCP/UDP - ICMP (Internet Control Message Protocol)
Destination IP Address	Destination IP address Format: xxx.xxx.xxx.xxx[/xx]

Table D-10: LAN > Networking Rules > Add Rule (Access Blocking) screen fields (Continued)

Field	Description
Destination Port Range	Starting and ending source port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port
Action	Action to take when traffic matches the rule's specifications: - Reject — Send the Reject Cause to the sender. - Drop — Drop the traffic packets without notice. <i>Note: The 'Drop' rule is useful when attempting to prevent hacking.</i>
Reject Cause	Reason that user receives when Action is set to 'Reject' - Prohibited — Inform user that site is banned. - Unreachable — Inform user that site is unreachable.

Access Granting Rules

Add an Access Granting rule to permit incoming or outgoing traffic (from the MG90's perspective) for a specific IP address, based on the criteria in [Table D-11](#) on page 160.

Tip: Fields that are left blank are treated as "wildcards." Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.

Note: By default, all ports (except ports 22 and 2222 (SSH)) to the MG90 from the WAN side are blocked. Access granting rules will not open additional ports to the MG90 but are designed to act as exceptions to access blocking rules.

The screenshot shows the 'Access Granting Firewall Rule' configuration window. The title bar indicates it's for 'LAN Global Rules'. The 'Rule Name' field contains 'Test Global Granting Rule #1'. The 'Direction' is set to 'Outgoing'. The 'Source IP Address' is '192.168.1.240/32'. The 'Source Port Range' is '100' to '104'. The 'Protocol' is 'TCP'. The 'Destination IP Address' is '192.168.15.72/32'. The 'Destination Port Range' is '110' to '114'. At the bottom, there are 'Save' and 'Cancel' buttons.

Figure D-11: LCI: LAN > Networking Rules > Add Rule (Access Granting)—Sample screen

Table D-11: LAN > Networking Rules > Add Rule (Access Granting) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.
Direction	Traffic direction relative to the MG90 - Incoming — The Source IP Address will be granted access. - Outgoing — The Destination IP Address will be granted access.

Table D-11: LAN > Networking Rules > Add Rule (Access Granting) screen fields (Continued)

Field	Description
Source IP Address	Source IP address - Format: [!]<i>xxx.xxx.xxx.xxx</i>[/<i>xx</i>] - Note: The optional '!' means "anything other than this address (or range)". - Examples: - Address without netmask—192.168.4.17. Applies to the stated IP address. - Address with netmask—192.168.4.0/24. Applies to the IP address range 192.168.4.0–192.168.4.255.
Source Port Range	Starting and ending source port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port
Protocol	Communications protocol - TCP - UDP - TCP/UDP - ICMP (Internet Control Message Protocol)
Destination IP Address	Destination IP address - Format: [!]<i>xxx.xxx.xxx.xxx</i>[/<i>xx</i>] - Note: The optional '!' means "anything other than this address (or range)".
Destination Port Range	Starting and ending source port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port

QoS Priority Rules

Add QoS Priority rules to various applications used by the customer and guarantee a certain level of performance to data flow.

Tip: Fields that are left blank are treated as "wildcards". Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.

For applications that do not have a predetermined destination IP address such as Voice-over-IP, using the Source IP Address and Source Port is supported.

QoS Priority Rule
(LAN Global Rules)

Rule Name: LAN Global Rule #1

Destination Address/Netmask: 208.81.125.0/24 CIDR notation a.b.c.d[/x]

Destination Port Range: Start 2048 End(Optional) 4096

Protocol: TCP/UDP

Source Address/Netmask: 10.1.60.0/24 CIDR notation a.b.c.d[/x]

Source Port Range: Start 2048 End(Optional) 4096

Priority: 0 Smaller numbers have greater priority

DSCP Value: EF Default is CS0 (IP precedence 0)

Minimum Guaranteed Bandwidth: ☒ No guarantee
☐ Rate 0 B/s

Maximum Allowed Bandwidth: ☒ Use available
☐ Rate 0 B/s

Save Cancel

Figure D-12: LCI: LAN > Networking Rules > Add Rule (QoS Prioritizing)—Sample screen

Table D-12: LAN > Networking Rules > Add Rule (QoS Prioritizing) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule
Destination Address/Netmask	Application server IP address - Format: [!]xxx.xxx.xxx.xxx[/xx] (CIDR notation) - Note: The optional '!' means "anything other than this address (or range)". - Leaving this field blank gives priority to all traffic on this port, based on existing firewall rules.
Destination Port Range	Destination port number (For TCP, UDP, TCP/UDP Protocols) - Single port used for data transport (Start), or range of ports (Start/End) - End port is Optional - Valid values: 0–65535 <i>Note: This field is available only if Protocol type is TCP, UDP, or TCP/UDP.</i>
Protocol	Data transport protocol - ALL - TCP/UDP - TCP - UDP - ICMP
Source Address/Netmask	Source IP address (used for applications that do not have a predetermined IP address (e.g. VoIP)) - Format: [!]xxx.xxx.xxx.xxx[/xx] (CIDR notation) - Note: The optional '!' means "anything other than this address (or range)".
Source Port Range	Source port number (used for applications that do not have a predetermined IP address (e.g. VoIP)) - Single port used for data transport (Start), or range of ports (Start/End) - End port is Optional - Valid values: 0–65535 <i>Note: This field is available only if Protocol type is TCP, UDP, or TCP/UDP.</i>

Table D-12: LAN > Networking Rules > Add Rule (QoS Prioritizing) screen fields (Continued)

Field	Description
Priority	Traffic priority Traffic to the WAN in the specified port and destination IP address is prioritized using this value. - Format: Integer - Minimum value: 0 (Highest priority) - Higher values are lower priority
DSCP Value	DSCP (Differentiated Services Code Point), also known as PNTM (Private Network Traffic Management) for Verizon - Select appropriate DSCP value from list. For DSCP details, refer to RFC 2597 and RFC 3260. - Values in the list are sorted from lowest priority (CS0) to highest priority (EF). - Value is used to prioritize traffic for end-to-end QoS across all devices in the path (if DSCP is supported).
Minimum Guaranteed Bandwidth	Minimum data transfer rate - No guarantee — No minimum data transfer rate. (Default) - Rate — Specify the minimum data rate (including the transfer unit) that should be provided <i>Note: If minimum bandwidth is specified for some rules, consider adding it to all rules. When the sum of the minimum guaranteed bandwidths for all transmissions is greater than the available bandwidth, transmissions with no guarantee will be stalled.</i>
Maximum Allowed Bandwidth	Maximum data transfer rate - Use available — No maximum data rate. (Default) - Rate — Specify the maximum data rate (including the transfer unit) that can be used. The maximum allowed bandwidth is used to ensure that traffic matching the condition specified by the rule does not exceed this bandwidth.

D.6 LAN > LAN Throughput

The LAN Throughput tab is used to configure throughput event reporting for specific ports. These event reports are sent to AMM, which then uses them for various reports.

A throughput report event is generated when:

- The throughput Threshold has been reached and the Minimum Report Interval has elapsed
- The Maximum Report Interval has elapsed

Figure D-13: LCI: LAN > LAN Throughput—Sample screen

Table D-13: LAN > LAN Throughput screen fields

Field	Description
Minimum Report Interval (Secs)	Minimum time between throughput report events Reports are not generated more often than this value. Default: 60 seconds (1 minute)
Maximum Report Interval (Secs)	Maximum time between throughput report events A report will be generated after this interval even if the throughput Threshold limit has not been reached. Default: 900 seconds (15 minutes)
Threshold (KiB)	Throughput report event threshold Throughput report event is generated when this threshold has been reached and the Minimum Report Interval has passed. Default: 1024 KiB (1 MB)
Monitored Ports (Separated by Space)	Ports being monitored for throughput Throughput on the listed ports is monitored and reported based on the other throughput configuration fields. - Default port: 80 - Multiple ports must be separated by spaces

D.7 LAN > Captive Portal

The Captive Portal tab lists all defined captive portals. For a description of the Captive Portal feature, see [Setting up Captive Portals](#) on page 70.

Friendly Name	Type	Actions
Conference Center Premium	Captive Portal	Delete Configure
Hotel Portal	Captive Portal	Delete Configure

[Add New Captive Portal Configuration](#)

Figure D-14: LCI: LAN > Captive Portal—Sample screen

Table D-14: LAN > Captive Portal screen fields

Field	Description
Friendly Name	Descriptive name for the captive portal. To change the description, see LAN > Captive Portal > Configure on page 165.
Type	"Captive Portal" (No other value will appear)
Actions	Click these optional links to perform actions on the associated captive portal: - Delete — Delete the associated captive portal. - Configure — Click to configure the captive portal. See LAN > Captive Portal > Configure on page 165.

D.8 LAN > Captive Portal > Configure

The Captive Portal Configuration screen is used to configure and enable/disable a captive portal hotspot (“walled garden”). A Wi-Fi module on the MG90 that has been set up as an access point can be configured (if desired) to use any one of the defined captive portals.

Captive Portal support requires that only one Wi-Fi module is configured as an access point.

Captive portals can be hosted by an external portal server, or by the MG90 using its built-in ‘miniportal’.

The screenshot displays the 'Captive Portal Configuration' screen. At the top, there is a navigation bar with tabs: Status, Devices, Security, LAN (selected), WAN, GPS, General, Logs, Applications, and Logout. Below this, a sub-bar shows: Ethernet Links, Access Points, LAN Segments, Virtual LANs, Networking Rules, LAN Throughput, and Captive Portal (selected).

The main configuration area is titled 'Captive Portal Configuration'. It includes the following sections:

- Enable:** A checkbox that is checked.
- Friendly Name:** A text field containing 'Conference Center Premium'.
- Network:** A text field containing '192.168.0.0'.
- Netmask:** A text field containing '255.255.255.0'.
- Gateway IP:** A text field containing '192.168.0.1'.
- UAM Port:** A text field containing '3990'.
- UAM UI Port:** A text field containing '4990'.
- UAM Secret:** A text field.
- NASID:** A text field.
- Auto DNS:** A checkbox that is checked.
- Primary DNS:** A text field containing '192.168.0.1'.
- Secondary DNS:** A text field.
- Session Timeout:** A text field containing '0' with a unit of 'Seconds'.
- Idle Timeout:** A text field containing '0' with a unit of 'Seconds'.
- Max Download Speed:** A text field containing '0' with a unit of 'bps'.
- Max Upload Speed:** A text field containing '0' with a unit of 'bps'.
- Miniportal Register Mode:** A dropdown menu set to 'Not set'.
- 802.1x Radius Servers:** A section with two columns: 'Primary' and 'Secondary'. Each column has fields for Address, Authentication Port (1812), Accounting Port (1813), and Secret.
- UAM Domains:** A text field containing '.paypal.com, paypalobjects.com' with a 'Comma separated' note.
- UAM Server:** A text field containing '\$HS_UAMLISTEN'.
- UAM Format:** A text field containing 'http://\$HS_UAMLISTEN:\$HS_UAMUIPORT/www/login.chi' with an 'Actual captive portal URL' note.
- UAM Homepage:** A text field containing 'http://\$HS_UAMLISTEN:\$HS_UAMPORT/www/coova.html'.
- URL White List:** A text field containing '\$HS_UAMLISTEN,\$HS_DNS1,\$HS_RADIUS,\$HS_UAMSERVER,\$HS_DNS2,\$HS_RADIUS2' with a 'Comma separated' note.
- Mac Authentication Mode:** A dropdown menu set to 'server' with a note: 'If "server" is specified, Local MAC WhiteList is ignored'.
- Local MAC WhiteList Format:** A text field containing '00-0A-5E-AC-BE-51' with a 'Comma separated' note.

Figure D-15: LCI: LAN > Captive Portal—Sample screen

Table D-15: LAN > Captive Portal screen fields

Field	Description
Enable	Enable/disable this Captive Portal When a user connects to an access point associated with this portal (LAN > Access Points on page 144), if this option is: - Selected — The captive portal is enabled, and users are automatically directed through it. - Not selected — The captive portal is disabled, and users connect directly to the WAN.
Friendly Name	Descriptive name that identifies the portal in LAN > Access Points.
Network	Internal IP address of the captive portal on the MG90. Example: 192.168.0.0 <i>Note:</i> Internally, this value is assigned to the variable <code>\$HS_UAMLISTEN</code>.

Table D-15: LAN > Captive Portal screen fields (Continued)

Field	Description
Netmask	Netmask that defines the LAN segment based on the Network Example: 255.255.255.0 is a "/24" netmask. If the Network field is 192.168.0.0 and the Gateway IP is 192.168.0.1, devices connecting to the captive portal will be assigned addresses in the range 192.168.0.2 – 192.168.0.255.
Gateway IP	Captive portal's IP address on subscriber network. The address is limited to a value in the range defined by the Network and Netmask Example: If Network is 192.168.0.0 and Netmask is 255.255.255.0, the Gateway IP must be in the range 192.168.0.1 through 192.168.0.255.
UAM Port	Captive portal's UAM (Universal Access Mode) port on subscriber network. Use the default value (3990) unless otherwise instructed.
UAM UI Port	Captive portal's UAM "UI" port on subscriber network, for embedded portal. Use the default value (4990) unless otherwise instructed.
UAM Secret	(External portals only) Password assigned by the external portal server that hosts the captive portal.
NASID	(External portals only) Unique value assigned to the MG90 by the external portal server to identify the device to backend systems.
Auto DNS	DNS (Domain Name Server) used for the captive portal - Selected — MG90's DNS is used. (Primary DNS and Secondary DNS fields are ignored.) - Not selected — External DNS server is used.
Primary DNS	IP address of preferred DNS server to use <i>Note: This field is available only if Auto DNS is selected.</i>
Secondary DNS	IP address of alternate DNS server to use if Primary DNS is unavailable <i>Note: This field is available only if Auto DNS is selected.</i>
Session Timeout	Maximum time a session can stay open before automatically ending 0 — No time limit ≥1 — Session times out after this many seconds
Idle Timeout	Maximum time a session can remain idle before automatically ending 0 — No time limit ≥1 — Session times out after being idle for this many seconds
Max Download Speed	Maximum download speed 0 — No limit (can use all available bandwidth) ≥1 — Maximum download speed in bits per second
Max Upload Speed	Maximum upload speed 0 — No limit (can use all available bandwidth) ≥1 — Maximum upload speed in bits per second
Miniportal Register Mode	Captive Portal provider - Not set — Use an external portal server - self — Use the MG90's built-in 'miniportal' server

Table D-15: LAN > Captive Portal screen fields (Continued)

Field	Description
802.1x Radius Servers	
RADIUS (Remote Authentication Dial-In User Service) servers used to authenticate and authorize users who attempt to access the captive portal. If two servers are used, captive portal access can be authorized if one server becomes unavailable.	
Primary	
Address	IP address of the primary RADIUS authentication/accounting server
Authentication Port	Server port used for authentication. Use the default port (1812) unless instructed otherwise.
Accounting Port	Server port used for accounting. Use the default port (1813) unless instructed otherwise.
Secret	Shared secret code required to access the RADIUS server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
Secondary	
Address	IP address of the secondary authentication/accounting server
Authentication Port	Server port used for authentication. Use the default port (1812) unless instructed otherwise.
Accounting Port	Server port used for accounting. Use the default port (1813) unless instructed otherwise.
Secret	Shared secret code required to access the RADIUS server from the MG90. If the shared secret is incorrect, the server ignores authentication requests.
UAM Domains	Comma-separated list of domain names that can be accessed via the captive portal page before the user is approved. For example, if the captive portal has a paid tier of services, the user must be able to connect through to an appropriate payment site. If the payment site is not in this list, the portal would prevent it from being accessed. Use the default list (.paypal.com,.paypalobjects.com) to allow users to pay for service using paypal, or add additional domains to use other services.
UAM Server	Hostname of captive portal server Use the default value unless otherwise instructed.
UAM Format	URL of captive portal Use the default value unless otherwise instructed.
UAM Homepage	Captive portal main page (e.g. login page) Use the default value unless otherwise instructed.
URL White List	Comma-separated list of URLs that user can be redirected to by the captive portal server for authentication, accounting, for free (unauthenticated) access, etc. Some examples include: ▪ RADIUS servers must be included (if used). ▪ Corporate page (for example, the public site for a hotel chain that is providing the hotspot) Use the default value unless otherwise instructed.

Table D-15: LAN > Captive Portal screen fields (Continued)

Field	Description
Mac Authentication Mode	Enable/disable authentication of specific devices using their MAC addresses - off — Device MAC addresses are not used to authenticate users. - local — Local MAC Whitelist is enabled. - server — MAC authentication is provided by the RADIUS server to allow access by specific devices (the list is maintained on the server).The Local MAC Whitelist is ignored
Local MAC Whitelist Format: 00-0A-5E-AC-BE-51	Comma-separated list of MAC addresses of devices that are automatically authenticated to access the portal.

E: WAN Tab

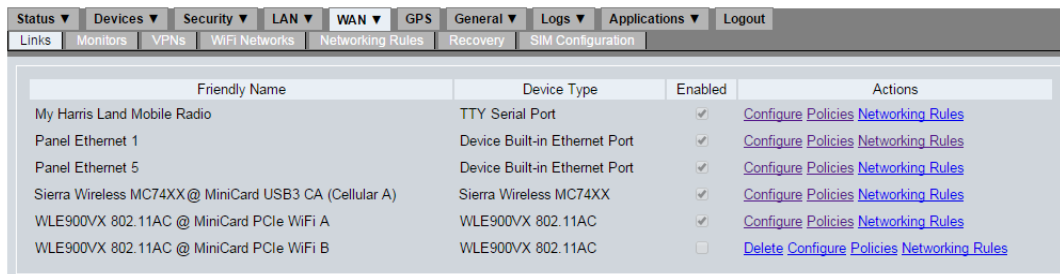
This chapter describes the WAN tab, which is used to configure the MG90's WAN interfaces — cellular, Wi-Fi, Ethernet, and serial modem.

The WAN tab includes the following sub-tabs:

- **Links** — Configure the MG90's WAN-capable devices for WAN use. See [WAN > Links](#) on page 169.
- **Monitors** — Configure monitors to detect and recover from communication failures. See [WAN > Monitors](#) on page 199.
- **VPNs** — Configure VPNs to allow LAN devices connected to the MG90 to access an enterprise network and vice-versa. See [WAN > VPNs](#) on page 201.
- **WiFi Networks** — Configure the MG90 to access specific Wi-Fi networks / access points. See [WAN > WiFi Networks](#) on page 210.
- **Networking Rules** — Configure rules to block or permit specific devices on the WAN, to perform port forwarding, and to ensure quality of service. See [WAN > Networking Rules](#) on page 220.
- **Recovery** — Configure the MG90 to recover from dead WAN connections. See [WAN > Recovery](#) on page 228.
- **SIM Configuration** — Indicate which SIM slots to use for the cellular radios. See [WAN > SIM Configuration](#) on page 229.

E.1 WAN > Links

Each device that can be, or has been used as a WAN connection is called a WAN 'link'. This screen displays all WAN links and the available Actions for configuring them.



Friendly Name	Device Type	Enabled	Actions
My Harris Land Mobile Radio	TTY Serial Port	☒	Configure Policies Networking Rules
Panel Ethernet 1	Device Built-in Ethernet Port	☒	Configure Policies Networking Rules
Panel Ethernet 5	Device Built-in Ethernet Port	☒	Configure Policies Networking Rules
Sierra Wireless MC74XX @ MiniCard USB3 CA (Cellular A)	Sierra Wireless MC74XX	☒	Configure Policies Networking Rules
WLE900VX 802.11AC @ MiniCard PCIe WiFi A	WLE900VX 802.11AC	☒	Configure Policies Networking Rules
WLE900VX 802.11AC @ MiniCard PCIe WiFi B	WLE900VX 802.11AC	☐	Delete Configure Policies Networking Rules

Figure E-1: LCI: WAN > Links—Sample screen

Table E-1: WAN > Links screen fields

Field	Description
Friendly Name	Descriptive device names defined in Devices tabs (Devices > Cellular, etc.)
Device Type	Hardware device type (cannot be modified)
Enabled	Indicates whether the device is currently enabled as a WAN link: - Selected — Device is available and selected for WAN usage. - Not selected — Device is either currently assigned for LAN usage, idle, or has been removed from the MG90.

Table E-1: WAN > Links screen fields (Continued)

Field	Description
Actions	Click these optional links to perform actions on the associated WAN links: ▪ Delete — Delete the associated WAN link (including its configuration details, policy assignments, and networking rules.). This option does not appear if the link is Enabled. <i>Caution: The link is deleted immediately. If you delete a link in error, you will have to re-enter any appropriate configurations, policies, and networking rules.</i> ▪ Configure — Configure link-specific details (IP addresses, monitors, etc.). See WAN Link Configuration (WAN > Links > Configure) on page 170. ▪ Policies — Configure link-specific policies used to determine which link is active. See WAN Link Policy Configuration (WAN > Links > Policies) on page 190. ▪ Networking Rules — Create networking rules (access granting, access blocking, port forwarding, QoS prioritizing). See WAN > Networking Rules on page 220.

E.1.1 WAN Link Configuration (WAN > Links > Configure)

The WAN Link Configuration screen that appears when you click Configure in the WAN > Links screen depends on the associated WAN link type:

- Ethernet — See [Ethernet WAN Link Configuration](#) on page 171
- Cellular — See [Cellular WAN Link Configuration](#) on page 176
- Wi-Fi — See [Wi-Fi WAN Link Configuration](#) on page 184
- Serial modem — See [Serial \(Modem\) WAN Link Configuration](#) on page 185

Note: Several options appear in more than one link type, but must be set independently.

E.1.1.1 Ethernet WAN Link Configuration

Ethernet WAN Link Configuration
(Panel Ethernet 5)

High Cost Link ☐

Change Default MTU Size ☐

MTU Size

Auto Local IP ☒

DHCP Assumes Same Network ☐

Send Hostname with DHCP ☒ Disabled
☐ Send ESN
☐ Custom

Local IP Address

Network Mask

Gateway

Masquerade ☒

Masquerade Port Range ☐ Automatic
☒ Manual
 Minimum Port Number
 Maximum Port Number

Automatic DNS ☒

Primary DNS

Secondary DNS Servers comma-separated IP addresses

Enable Private Zone ☐

Number of Private Zone

Use Management Tunnel ☒

Pilot Ping ☐

Monitors ☒ DefaultMonitor

Monitor Mode

VPN ☒ VPN Configuration ☒ VPN Configuration_1 ☐ VPN Configuration_2

Connection Method ☒ Connect One
☐ Random
☐ Round Robin - Alphanumeric Order
☐ Connect All

Load Balanced ☐

Weight (1-256)

Split Access ☐

Save Cancel

Figure E-2: LCI: WAN > Links > Configure (Ethernet)—Sample screen

Table E-2: WAN > Links > Configure (Ethernet) screen fields

Field	Description
High Cost Link	High Cost Link - Selected — High cost link. Transmission of management data (e.g. log files uploads, automatic software downloads, etc.) is limited, with most of the data being held until a low cost link is active. (Note: If required, you can allow Auto software updates and firmware updates over high cost links, by setting appropriate options. See Table G-8, General > Auto Software Updates screen fields, on page 248 for details.) - Not selected — Not a high cost link. <i>Note: Ethernet links are typically not high cost, while cellular links would typically be high cost (depending on the data plan type).</i>

Table E-2: WAN > Links > Configure (Ethernet) screen fields (Continued)

Field	Description
Change Default MTU Size	Use a different MTU Size than the default (1500 bytes) - Selected — MTU Size field can be edited. (Default) Deselect this checkbox to reset the MTU Size to the default value (the value resets when you click Save). - Not selected — MTU Size field cannot be edited. <i>Note: This may be required to accommodate some network configurations. Only change this value if instructed to by Sierra Wireless.</i>
MTU Size	Maximum Transmission Unit size (in bytes) - Valid range: 256–1500 - Default: 1500
Auto Local IP	Enable DHCP for this interface. - Selected — Enabled. The IP address will be assigned by a DHCP server connected to the access point network. - Not selected — Not enabled. Assign the Local IP Address, Network Mask, and Gateway manually.
DHCP Assumes Same Network	DHCP assignment when DHCP lease expires - Selected — Attempt to reconnect to same DHCP assignment when the lease expires. - Not selected — Gateway will request an IP address from a DHCP server in the available network when the lease expires. <i>Note: This field is available only if Auto Local IP is selected.</i>
Send Hostname with DHCP request	Enable / disable sending of MG90-identifying information with DHCP request - Disabled — Do not send identifying information - Send ESN — Send the MG90's ESN (Electronic Serial Number) - Custom — Send a custom hostname (for example, "Bus401") to identify the MG90 to the DHCP server. <i>Note: This field is available only if Auto Local IP is selected.</i>
Local IP Address	Statically-assigned Local IP Address IPv4 address format (e.g. xxx.xxx.xxx.xxx) <i>Note: This field is available only if Auto Local IP is not selected.</i>
Network Mask	Network mask of the Local IP Address IPv4 netmask format (e.g. xxx.xxx.xxx.xxx) <i>Note: This field is available only if Auto Local IP is not selected.</i>
Gateway	Default gateway to use for the Local IP Address IPv4 address format (e.g. xxx.xxx.xxx.xxx) <i>Note: This field is available only if Auto Local IP is not selected.</i>
Masquerade	Network Address Translation for LAN-originated traffic leaving the MG90 WAN interface - Selected — Enabled. This is the typical setting. - Not selected — Disabled

Table E-2: WAN > Links > Configure (Ethernet) screen fields (Continued)

Field	Description
Masquerade Port Range	Port range to use for masquerade (NAT) - Automatic — Enabled - Manual — Disabled (Default). This should be used in most cases to avoid using defined or reserved ports. <i>Note: This field is available only if Masquerade is selected.</i>
Minimum Port Number	Range of ports to use for masquerade (NAT) Default range: 49152–65535
Maximum Port Number	- Valid range: 0–65535 - If Minimum Port Number < 49152: - traffic on ports lower than 512 is mapped to other ports lower than 512 - traffic on ports 512 to 1024 is mapped to ports lower than 1024 - traffic on ports greater than 1024 is mapped to ports greater than 1024 <i>Note: These fields are available only if Masquerade is selected and Masquerade Port Range is Manual.</i>
Automatic DNS	DNS servers to be used - Selected — Use DNS servers specified by DHCP server. - Not selected — Use the DNS servers specified in Primary DNS or Secondary DNS. The fastest-responding server (regardless of whether named as Primary or Secondary) is chosen as the server to use. Periodically, the servers are re-evaluated to make sure the fastest-responding server is being used. If private DNS servers are used, set up DNS zones — see Configuring DNS Zones for Private DNS Server Use on page 82 for details. <i>Note: This must be disabled (not selected) if using a static IP address.</i>
Primary DNS	IP address of primary domain name server - Format: IPv4 address (xxx.xxx.xxx.xxx) - Required field (when Automatic DNS is not selected) <i>Note: This field is available only if Automatic DNS is not selected.</i>
Secondary DNS Servers	IP addresses of secondary domain name servers - Format: IPv4 addresses, comma-separated (e.g. xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy) - Optional field <i>Note: This field is available only if Automatic DNS is not selected.</i>
Enable Private Zone	Enables/disables DNS private zone use on this link. - Selected — Enabled. DNS private zones can be used on this link. - Not selected — Disabled. DNS private zones cannot be used on this link.
Number of Private Zone	Table of 1–10 private zone configuration entries
Private Zone <#>	Domain name to be resolved by the internal DNS server managing the private zone.
Private Zone IP <#>	IP address of the internal DNS server managing the private zone.

Table E-2: WAN > Links > Configure (Ethernet) screen fields (Continued)

Field	Description
Use Management Tunnel	Management Tunnel usage The management tunnel is a dedicated secure VPN connection between the MG90 and AMM. - Selected — AMM can access the MG90. (Default) - Not selected — Do not use the management tunnel. AMM cannot access the MG90. To configure the management tunnel, see WAN > VPNs > (Management Tunnel) > Configure on page 202.
Pilot Ping	Pilot ping - Selected — Enabled. Before a WAN link is identified as established, the MG90 attempts to pass ping traffic over the link. If the ping succeeds, the link is identified as established. If the ping fails, the link is not established. - Not selected — Disabled (Default). Ping traffic is not attempted, which could result in a WAN link being identified as established although it may not be able to pass traffic. <i>Note: After a WAN link has been established, ping monitors (next field) are used to monitor the link's connection.</i>
Monitors	Monitor(s) being used to monitor the link's connection state Select one or more monitors. Factory-defined monitor — DefaultMonitor. This example should be replaced with your own monitor definition. To configure monitors, see WAN > Monitors > Configure on page 200.
Monitor Mode	Effect of selected monitors' state on link status - Success in one monitor keeps the link up — If at least one monitor is reporting as active, then the link should be considered 'up'. - Failure in one monitor declares the link down — If any one monitor is reporting as inactive, then the link should be considered 'down'. <i>Note: This field is meaningful only if one or more monitors are selected.</i>
VPN	VPNs that the WAN link can establish when the link is active If multiple VPNs are selected, each must be LAN to LAN. To configure VPNs, see WAN > VPNs on page 201. Warning: In the VPN field, if a VPN profile is selected that is configured as a full tunnel (subnet 0.0.0.0/0), do not select any other profiles. If the full tunnel profile and another profile are selected, none of the changes made to the screen will be saved when Save is clicked.
Connection Method	Number of VPN tunnels to establish for a WAN connection - Connect One — Only 1 tunnel established for the WAN link, using selected method below: - Random — Establish tunnel on a randomly selected VPN from the VPN list. If tunnel cannot be established or fails, use next randomly selected VPN. This results in basic (unmanaged) load balancing across VPN servers. - Round Robin - Alphanumeric Order — Establish tunnel on the first VPN (sorted by name) in the VPN list. If tunnel cannot be established or fails, use next VPN (in sorted order). This is a redundant failover method that does not have any load-balancing characteristics. - Connect All — Tunnels to all VPNs in the VPN list established simultaneously for the WAN link. <i>Note: This option (Connect All) can only be selected for LAN-to-LAN VPNs.</i> <i>Note: Any changes to Connection Method take effect after the next reboot.</i>

Table E-2: WAN > Links > Configure (Ethernet) screen fields (Continued)

Field	Description
Load Balanced	Distribute traffic across active WAN links When load balancing is selected on two or more active WAN links, traffic can be distributed across these links (based on their Weight field values). - Selected — Distribute traffic across links, based on Weight field values. - Not selected — Do not load balance See Configuring Load Balancing on page 74 for usage.
Weight (1-256)	Load balancing 'weight' When load balancing is enabled on two or more links, their Weights are used to calculate the proportion of traffic each link will receive: $\text{Proportion (Link)} = \text{Weight (Link)} / \text{Total_Weight (All Links)}$ For example: Link A Weight = 50 Link B Weight = 100 Proportion (Link A) = $50 / (50 + 100) = 33.3\%$ Proportion (Link B) = $100 / (50 + 100) = 66.7\%$ Therefore, Link B will carry twice as many sessions as Link A. <i>Note: This field is available only if Load Balanced is selected.</i>
Split Access	Allow incoming session initiation on non-active connected link This allows an incoming session to initiate on a link even when the link is not the active (i.e. default route) link but is connected to the network. - Selected — Allowed - Not selected — Not allowed This is useful for test purposes on Ethernet links that have public IP addresses. It also enables applications such as live video look-in to an Ethernet interface even if the active connection is via another WAN (e.g. Wi-Fi). <i>Note: Users are encouraged to evaluate use of the Split Access feature from a security and system perspective prior to enabling. Depending on available links and routing rules, traffic may route from WAN to LAN or between WAN networks.</i>

E.1.1.2 Cellular WAN Link Configuration

The screenshot displays the 'Cellular WAN Link Configuration' window for a 'Sierra Wireless MC74XX @ MiniCard USB3 CA (Cellular A)' device. The interface includes a top navigation bar with tabs for Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below this is a sub-navigation bar with tabs for Links, Monitors, VPNs, WiFi Networks, Networking Rules, Recovery, and SIM Configuration. The main configuration area is divided into two columns. The left column lists various settings, and the right column provides the corresponding input fields or options. Key settings include: High Cost Link (unchecked), MTU Size (Automatic), Enable TCP MSS Clamping (checked), Masquerade (checked), Masquerade Port Range (Manual, with Minimum Port Number 49152 and Maximum Port Number 65535), Automatic DNS (checked), Primary DNS (empty), Secondary DNS Servers (empty), Enable Private Zone (unchecked), Number of Private Zone (1), APN (sp.telus.com), Allow Blank APN (unchecked), Signal Strength Filter Length (10), Signal Strength Change Threshold (dBm) (5), Setting for Band (All Bands), Custom Band Setting Mode (Exclude Bands, with 4 comma-separated bands), Use Management Tunnel (checked), Pilot Ping (unchecked), Monitors (checked, DefaultMonitor), Monitor Mode (Success in one monitor keeps the link up), VPN (unchecked), Connection Method (Connect All), Load Balanced (unchecked), Weight (1-256) (1), Split Access (unchecked), Enable Advanced Module Recovery (checked, with Recovery Interval of 10 minutes), Advanced Modem Initialization (~), Preferred Mode (Automatic), and Enable IPV6 (unchecked). At the bottom right, there are 'Save' and 'Cancel' buttons.

Setting	Value/Option
High Cost Link	☐
MTU Size	☒ Automatic ☐ Manual
Enable TCP MSS Clamping	☒
Masquerade	☒
Masquerade Port Range	☐ Automatic ☒ Manual Minimum Port Number: 49152 Maximum Port Number: 65535
Automatic DNS	☒
Primary DNS	
Secondary DNS Servers	comma-separated IP addresses
Enable Private Zone	☐
Number of Private Zone:	1
APN	sp.telus.com
Allow Blank APN	☐
Signal Strength Filter Length	10
Signal Strength Change Threshold (dBm)	5
Setting for Band	All Bands
Custom Band Setting Mode	Exclude Bands 4 comma-separated bands
Use Management Tunnel	☒
Pilot Ping	☐
Monitors	☒ DefaultMonitor
Monitor Mode	Success in one monitor keeps the link up
VPN	☐ VPN Configuration ☐ VPN Configuration_1 ☐ VPN Configuration_2
Connection Method	☐ Connect One ☐ Random ☐ Round Robin - Alphanumeric Order ☒ Connect All
Load Balanced	☐
Weight (1-256)	1
Split Access	☐
Enable Advanced Module Recovery	☒
Recovery Interval (minutes)	10
Advanced Modem Initialization	~ Comma separated
Preferred Mode	☒ Automatic ☐ LTE Disabled
Enable IPV6	☐

Figure E-3: LCI: WAN > Links > Configure (Cellular)—4G Cellular Sample screen

Status ▾ Devices ▾ Security ▾ LAN ▾ **WAN ▾** GPS ▾ General ▾ Logs ▾ Applications ▾ Logout
 Links Monitors VPNs WiFi Networks Networking Rules Recovery SIM Configuration

Cellular WAN Link Configuration

(Sierra Wireless EM919X @ MiniCard USB3 CA (Cellular A))

High Cost Link	☐
MTU Size	☒ Automatic ☐ Manual
Enable TCP MSS Clamping	☒
Masquerade	☒
Masquerade Port Range	☐ Automatic ☒ Manual Minimum Port Number 49152 Maximum Port Number 65535
Automatic DNS	☒
Primary DNS	
Secondary DNS Servers	comma-separated IP addresses
Enable Private Zone	☐
Number of Private Zone:	1
APN	m2minternet.apn
Allow Blank APN	☐
Signal Strength Filter Length	10
Signal Strength Change Threshold (dBm)	5
Setting for Band	All Bands
Custom Band Setting Mode	Exclude Bands 4,12 comma-separated bands
Use Management Tunnel	☒
Pilot Ping	☐
Monitors	☒ DefaultMonitor
Monitor Mode	Success in one monitor keeps the link up
VPN	
Connection Method	☐ Connect One ☐ Random ☐ Round Robin - Alphanumeric Order ☐ Connect All
Load Balanced	☐
Weight (1-256)	1
Split Access	☐
Enable Advanced Module Recovery	☒
Recovery Interval (minutes)	10
Advanced Modem Initialization	~ Comma separated
Enable IPV6	☐
Network Type	Auto
MIMO Configuration	2x2

Save Cancel

Figure E-4: LCI: WAN > Links > Configure (Cellular)—5G Cellular Sample screen

Table E-3: WAN > Links > Configure (Cellular) screen fields

Field	Description														
High Cost Link	High Cost Link - Selected — High cost link. Transmission of management data (e.g. log files uploads, automatic software downloads, etc.) is limited, with most of the data being held until a low cost link is active. (Note: If required, you can allow Auto software updates and firmware updates over high cost links, by setting appropriate options. See Table G-8, General > Auto Software Updates screen fields, on page 248 for details.) <i>Note: During initial testing, avoid enabling this feature to ensure all management events are emitted. If data plan costs are a concern, enable this after the MG90 is put into operation.</i> - Not selected — Not a high cost link. <i>Note: Cellular links are typically high cost (depending on the data plan type), while Ethernet links are typically not high cost.</i>														
MTU Size	Maximum Transmission Unit size (in bytes) - Automatic — Use the MTU size reported by the carrier during link negotiation or, if not provided, then use the network carrier's default MTU. <table border="1"> <thead> <tr> <th>Carrier</th><th>Default MTU Size</th></tr> </thead> <tbody> <tr> <td>AT&T</td><td>1430</td></tr> <tr> <td>FirstNet</td><td>1342</td></tr> <tr> <td>Generic</td><td>1430</td></tr> <tr> <td>Sprint</td><td>1422</td></tr> <tr> <td>Telstra</td><td>1358</td></tr> <tr> <td>Verizon</td><td>1428</td></tr> </tbody> </table> - Manual — Enter the MTU size - Valid range: 256–1500	Carrier	Default MTU Size	AT&T	1430	FirstNet	1342	Generic	1430	Sprint	1422	Telstra	1358	Verizon	1428
Carrier	Default MTU Size														
AT&T	1430														
FirstNet	1342														
Generic	1430														
Sprint	1422														
Telstra	1358														
Verizon	1428														
Enable TCP MSS Clamping	MSS (Maximum TCP Segment Size) Clamping controls the maximum packet size used for TCP connections between a local (LAN-side) host and a remote host over the cellular WAN interface. MSS Clamping helps avoid possible issues with sending and receiving large TCP packets over the cellular network when other standard MTU mechanisms do not appear to be working with your installation. Options are: - Selected (default) — MSS is clamped at MTU Size minus 40 bytes. - Not selected — Clamping is disabled. MSS defaults to 536 bytes.														
Masquerade	Network Address Translation for LAN-originated traffic leaving MG90 WAN interface - Selected — Enabled. This is the typical setting, since many carriers will disconnect a cellular modem that emits IP datagrams bearing an address other than that of the cellular modem. - Not selected — Disabled														
Masquerade Port Range	Port range to use for masquerade (NAT) - Automatic — Enabled - Manual — Disabled (Default). This should be used in most cases to avoid using defined or reserved ports. <i>Note: This field is available only if Masquerade is selected.</i>														

Table E-3: WAN > Links > Configure (Cellular) screen fields (Continued)

Field	Description
Minimum Port Number	Range of ports to use for masquerade (NAT)
Maximum Port Number	- Default range: 49152–65535 - Valid range: 0–65535 - If Minimum Port Number < 49152: - traffic on ports lower than 512 is mapped to other ports lower than 512 - traffic on ports 512 to 1024 is mapped to ports lower than 1024 - traffic on ports greater than 1024 is mapped to ports greater than 1024 <i>Note: These fields are available only if Masquerade is selected and Masquerade Port Range is Manual.</i>
Automatic DNS	DNS servers to be used - Selected — Use DNS servers specified by DHCP server. - Not selected — Use the DNS servers specified in Primary DNS or Secondary DNS. The fastest-responding server (regardless of whether named as Primary or Secondary) is chosen as the server to use. Periodically, the servers are re-evaluated to make sure the fastest-responding server is being used. If private DNS servers are used, set up DNS zones — see Configuring DNS Zones for Private DNS Server Use on page 82 for details. <i>Note: This must be disabled (not selected) if using a static IP address.</i>
Primary DNS	IP address of primary domain name server - Format: IPv4 address (xxx.xxx.xxx.xxx) - Required field (when Automatic DNS is not selected) <i>Note: This field is available only if Automatic DNS is not selected.</i>
Secondary DNS Servers	IP addresses of secondary domain name servers - Format: IPv4 addresses, comma-separated (e.g. xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy) - Optional field <i>Note: This field is available only if Automatic DNS is not selected.</i>
Enable Private Zone	Enables / disable DNS private zone use on this link. - Selected — Enabled. DNS private zones can be used on this link. - Not selected — Disabled. DNS private zones cannot be used on this link.
Number of Private Zone	Table of 1–10 private zone configuration entries
Private Zone <#>	Domain name to be resolved by the internal DNS server managing the private zone.
Private Zone IP <#>	IP address of the internal DNS server managing the private zone.
APN	Access Point Name Mobile Network Operator's Access Point Name - Verizon / AT&T / Sprint — Typically left blank. The APN is determined automatically when the carrier SIM is inserted and can be seen in Status > WAN > Extended Status. - Other carriers — Obtain from the service provider and enter the value in this field.

Table E-3: WAN > Links > Configure (Cellular) screen fields (Continued)

Field	Description
Allow Blank APN	Allows a blank APN to be used - Selected - If the APN field is blank, the APN will be cleared from the radio module. - If the APN field is not blank, the APN field is used as normal. - Not selected — APN must be used with the installed SIM - If the APN field is blank, a carrier default APN will be used (if known by MGOS) - If the APN field is not blank, the APN field is used as normal.
Signal Strength Filter Length	Number of samples used to determine signal strength Signal strength is calculated as the average value of the samples collected.
Signal Strength Change Threshold (dBm)	If signal strength increases or decreases by more than this threshold value in a 2 second period, send an event to AMM. For example: - Check signal strength X at time T. - Check signal strength Y at time T+2. - If $\text{abs}[X - Y] > \text{Threshold}$, send event report to AMM.
Setting for Band	Radio Access Technologies (RATs) that may be used, if supported by the module - All Bands — All bands on all RATs supported by the module can be used. - UMTS ALL — Only UMTS bands can be used. - LTE ALL — Only LTE bands can be used. 5G NR ALL — Only 5G NR bands can be used. (Available on 5G radio modules only.)
Custom Band Setting Mode	Bands (for supported RATs) that may be used - Disable — All bands supported by the module for the selected RATs (Setting for Band) can be used. - Exclude Bands — All bands supported by the module for the selected RATs can be used, except for the list in the next field. - Restrict to Bands — Only the bands in the next field can be used, and only if supported by the module for the selected RATs.
(comma-separated bands)	Bands that can or cannot be used, based on the Custom Band Setting Mode. - Bands are entered as a comma-separated list. - Bands are entered as numeric values only. (i.e., 5G band n2 is entered as '2'). <i>Note: This field is available only if Custom Band Setting Mode is not 'Disable'.</i> <i>Note: Band numbers are not checked against module support. The user must make sure the correct band numbers are entered.</i>
Use Management Tunnel	Management Tunnel usage The management tunnel is a dedicated secure VPN connection between the MG90 and AMM. - Selected — AMM can access the MG90. (Default) - Not selected — Do not use the management tunnel. AMM cannot access the MG90. To configure the management tunnel, see WAN > VPNs > (Management Tunnel) > Configure on page 202.

Table E-3: WAN > Links > Configure (Cellular) screen fields (Continued)

Field	Description
Pilot Ping	Pilot ping - Selected — Enabled. Before a WAN link is identified as established, the MG90 attempts to pass ping traffic over the link. If the ping succeeds, the link is identified as established. If the ping fails, the link is not established. - Not selected — Disabled (Default). Ping traffic is not attempted, which could result in a WAN link being identified as established although it may not be able to pass traffic. <i>Note: After a WAN link has been established, ping monitors (next field) are used to monitor the link's connection.</i>
Monitors	Monitor(s) being used to monitor the link's connection state Select one or more monitors. Notes: Factory-defined monitor — DefaultMonitor. This example should be replaced with your own monitor definition. To configure monitors, see WAN > Monitors > Configure on page 200.
Monitor Mode	Effect of selected monitors' state on link status - Success in one monitor keeps the link up — If at least one monitor is reporting as active, then the link should be considered 'up'. - Failure in one monitor declares the link down — If any one monitor is reporting as inactive, then the link should be considered 'down'. <i>Note: This field is meaningful only if one or more monitors are selected.</i>
VPN	VPNs that the WAN link can establish when the link is active If multiple VPNs are selected, each must be LAN to LAN. To configure VPNs, see WAN > VPNs on page 201. Warning: In the VPN field, if a VPN profile is selected that is configured as a full tunnel (subnet 0.0.0.0/0), do not select any other profiles. If the full tunnel profile and another profile are selected, none of the changes made to the screen will be saved when Save is clicked.
Connection method	Number of VPN tunnels to establish for a WAN connection - Connect One — Only 1 tunnel established for the WAN link, using selected method below: - Random — Establish tunnel on a randomly selected VPN from the VPN list. If tunnel cannot be established or fails, use next randomly selected VPN. This results in basic (unmanaged) load balancing across VPN servers. - Round Robin - Alphanumeric Order — Establish tunnel on the first VPN (sorted by name) in the VPN list. If tunnel cannot be established or fails, use next VPN (in sorted order). This is a redundant failover method that does not have any load-balancing characteristics. - Connect All — Tunnels to all VPNs in the VPN list established simultaneously for the WAN link. <i>Note: This option (Connect All) can only be selected for LAN-to-LAN VPNs.</i> <i>Note: Any changes to Connection Method take effect after the next reboot.</i>
Load Balanced	Distribute traffic across active WAN links When load balancing is selected on two or more active WAN links, traffic can be distributed across these links (based on their Weight field values). - Selected — Distribute traffic across links, based on Weight field values. - Not selected — Do not load balance See Configuring Load Balancing on page 74 for usage.

Table E-3: WAN > Links > Configure (Cellular) screen fields (Continued)

Field	Description
Weight (1-256)	Load balancing 'weight' When load balancing is enabled on two or more links, their Weights are used to calculate the proportion of traffic each link will receive: $\text{Proportion (Link)} = \text{Weight (Link)} / \text{Total_Weight (All Links)}$ For example: Link A Weight = 50 Link B Weight = 100 Proportion (Link A) = $50 / (50 + 100) = 33.3\%$ Proportion (Link B) = $100 / (50 + 100) = 66.7\%$ Therefore, Link B will carry twice as many sessions as Link A. <i>Note: This field is available only if Load Balanced is not selected.</i>
Split Access	Allow incoming session initiation on non-active connected link This allows an incoming session to initiate on a link even when the link is not the active (i.e. default route) link but is connected to the network. - Selected — Allowed - Not selected — Not allowed This is useful for test purposes on cellular links that have public IP addresses. It also enables applications such as live video look-in to a cellular interface even if the active connection is via another WAN (e.g. Wi-Fi). <i>Note: Users are encouraged to evaluate use of the Split Access feature from a security and system perspective prior to enabling. Depending on available links and routing rules, traffic may route from WAN to LAN or between WAN networks.</i>
Enable Advanced Module Recovery	Reboot cellular radio module (e.g. MC7354, MC7430/MC7455, EM7511/EM7565, EM9190) if link down for too long - Not selected — Disabled (Default) When the link goes down, the module begins attempting to reconnect, with an increasing delay between connection attempts. 1st attempt — Immediately tries to reconnect. 2nd attempt — 6 second delay before attempt. 3rd attempt — 12 second delay 4th attempt — 1 minute delay + random (0–15 seconds) 5th attempt — 2 minute delay + random (0–30 seconds) 6th attempt — 8 minute delay + random (0–60 seconds) 7th attempt (and onward) — 15 minute delay + random (0–120 seconds) This method is useful when a large number of devices disconnect simultaneously (e.g. due to a carrier outage). Without the variable delays, all devices would attempt to reconnect at the same time. With the variable delays, the group of devices will attempt to reconnect at different times. - Selected — Enabled. The module reboots when the link goes down for longer than the Recovery Interval period.

Table E-3: WAN > Links > Configure (Cellular) screen fields (Continued)

Field	Description
Recovery Interval (minutes)	Maximum link recovery period (in minutes) If the link goes down for longer than this period, the radio module (e.g. MC7354, MC7430/MC7455, EM7511/EM7565, EM9190) will reboot. - Default: 10 (600 seconds) - Minimum: 1 (60 seconds) <i>Note: This field is available only if Enable Advanced Module Recovery is selected.</i>
Advanced Modem Initialization	<i>Important: This field should only be used under the direction of Sierra Wireless Technical Support staff, or as described below.</i> If the WAN link is a private network that requires a user name and password for access, enter the following command in the Advanced Modem Initialization String field: <code>AT\$QCPDPP=1\,1\,<password>\,<username></code> For example: <code>AT\$QCPDPP=1\,1\,3AD29482\,6045551234@static.carrier.ca</code>
Preferred Mode	Radio Access Technology (RAT) type to use - Automatic — Select the best RAT available - LTE Disabled — Do not use LTE (4G) <i>Note: This field is available only if the radio module is an MC7354.</i>
Enable IPV6	Enable (or disable) use of IPv6 addresses if required by mobile network provider: - Selected — IPv6 addresses supported - Not selected — IPv6 addresses not supported
Network Type	<i>Note: This field is available only for 5G radio modules.</i> Network types that module can connect to: - Auto — 5G and LTE. Module connects to best available network.(Default) 5G Only — Module can connect only to 5G networks. - LTE Only — Module can connect only to LTE networks. <i>Note: For some carriers, this list may not include all the possible values listed above.</i>
MIMO Configuration	<i>Note: This field is available only for 5G radio modules. The field is display-only for dual radio MG90 5Gs.</i> MIMO configuration for installed module(s): 2x2: - Installed module(s) use 2x2 MIMO - Band n41 automatically disabled 4x4: - Available only for single radio MG90 5G - Default value (after factory reset)

E.1.1.3 Wi-Fi WAN Link Configuration

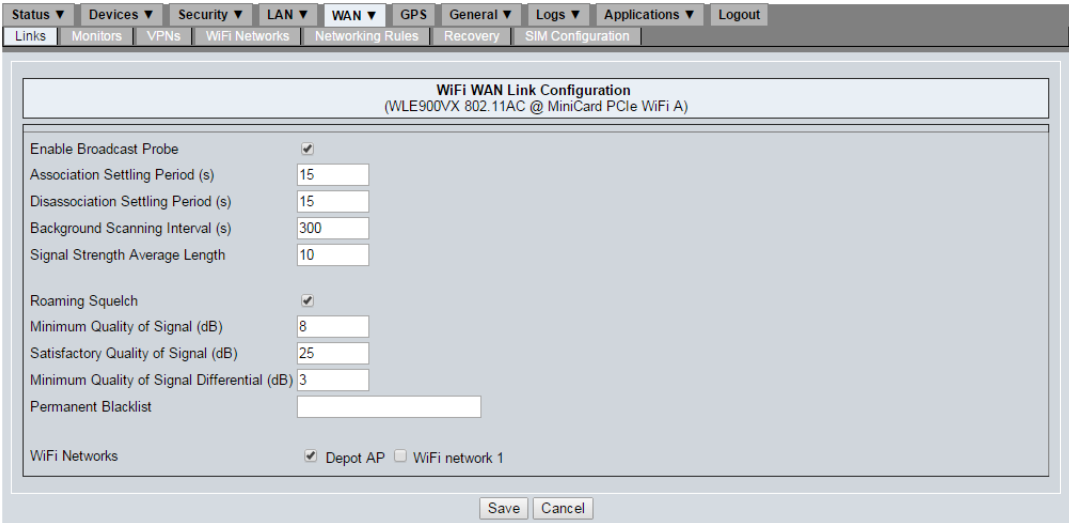


Figure E-5: LCI: WAN > Links > Configure (Wi-Fi)—Sample screen

Table E-4: WAN > Links > Configure (Wi-Fi) screen fields

Field	Description
Enable Broadcast Probe	Send periodic broadcast probe requests When enabled, a broadcast probe request is sent to all access points in the area. A probe request is sent by the client requesting information from either a specific access point or all access points in the area. - Selected — Probes enabled - Not selected — Probes not enabled
Association Settling Period (s)	Access Point Association Settling Period After connecting to a Wi-Fi access point, wait for this period (in seconds) before carrying traffic. This ensures that association to an AP with a marginal signal does not result in the link being selected for bearing default route traffic only to find it has disconnected. - Default: 15 - Recommended range: 1–60
Disassociation Settling Period (s)	Access Point Disassociation Settling Period When connected to a Wi-Fi access point and the link goes down, wait for this period (in seconds) before switching to another available link. The delay is intended to allow short interruptions to the Wi-Fi signal to be tolerated without provoking a link switch. - Default: 15 - Recommended range: 1–60

Table E-4: WAN > Links > Configure (Wi-Fi) screen fields (Continued)

Field	Description
Background Scanning Interval (s)	Interval between background scans for suitable access points Before associating successfully, a scan is continuously executed to look for access points with the appropriate credentials. Once associated, a background scan is executed on the interval defined by this parameter. The background scan allows the MG90 to detect nearby eligible APs. This value should be set moderately (e.g. 60 seconds) when in a depot environment and aggressively (e.g. every 2 seconds) when operating in metropolitan networks. Default: 300 (5 minutes)
Signal Strength Average Length	Number of background scan samples used to evaluate alternative APs This number of background scan samples are integrated to evaluate alternative APs. The default value of 10 readings is recommended for environments where there is only one access point with the appropriate credentials. For metropolitan networks, where the vehicle is expected to roam from access point to access point this value should be set to 1. Default: 10
Roaming Squelch	Prevent Roaming (subject to signal quality) If selected, the MG90 stays associated with an AP (i.e. will not roam) unless the AP is disqualified by the signal quality settings in the next three fields. - Selected — Do not roam. Typically used in a depot environment. - Not selected — Roam. Typically used in metropolitan network where fast roaming is required.
Minimum Quality of Signal (dB)	Minimum Access Point Signal to Noise Ratio (SNR) to establish association The MG90 will not associate to an AP unless its SNR meets or exceeds this value. (A low SNR usually implies a low signal.) SNR measured in dB <i>Note: This field is available only if Roaming Squelch is selected.</i>
Satisfactory Quality of Signal (dB)	Satisfactory Access Point Signal to Noise Ratio (SNR) to maintain association Once an MG90 has associated with an AP, it will remain associated unless the SNR drops below this value. SNR measured in dB <i>Note: This field is available only if Roaming Squelch is selected.</i>
Minimum Quality of Signal Differential (dB)	Minimum Signal to Noise Ratio (SNR) differential to support switching APs When the Wi-Fi interface is considering a switch to a new access point, the difference in signal SNR between the current access point and the new one must be greater or equal to this value. Differential measured in dB <i>Note: This field is available only if Roaming Squelch is selected.</i>
Permanent Blacklist	List of BSSIDs that the Wi-Fi interface should never connect to. One or more BSSIDs, comma-separated <i>Note: This field is available only if Roaming Squelch is selected.</i>
WiFi Networks	Wi-Fi networks that the link can connect to - Selected — Wi-Fi WAN link can connect to specified Wi-Fi network. - Not selected — Wi-Fi WAN link cannot connect to specified Wi-Fi network.

E.1.1.4 Serial (Modem) WAN Link Configuration

After adding a serial modem ([Configuring the Serial Port](#) on page 25), configure the WAN link that uses the device.

Serial WAN Link Configuration
(Harris Land Mobile Radio)

High Cost Link	☐
Change Default MTU Size	☐
MTU Size	1500
Auto Local IP	☒
Local IP Address	
Masquerade	☒
Masquerade Port Range	☐ Automatic ☒ Manual
Minimum Port Number	49152
Maximum Port Number	65535
Automatic DNS	☒
Primary DNS	
Secondary DNS Servers	comma-separated IP addresses
Auto Remote IP	☒
Remote IP Address	
Serial Modem Speed (bauds)	19200
Modem Initialization	~
Dial String	
Use Management Tunnel	☒
Pilot Ping	☐
Monitors	☒ DefaultMonitor
Monitor Mode	Success in one monitor keeps the link up
Call Down Recovery	☐
Recovery Time (seconds)	600
VPN	☐ VPN Configuration ☐ VPN Configuration_1 ☐ VPN Configuration_2
Connection Method	☐ Connect One ☐ Random ☐ Round Robin - Alphanumeric Order ☒ Connect All
Enable Custom txqueuelen	☐
txqueuelen value	10

Save Cancel

Figure E-6: LCI: WAN > Links > Configure (Serial (modem))—Sample Screen

Table E-5: WAN > Links > Configure (Serial (modem)) screen fields

Field	Description
High Cost Link	High Cost Link - Selected — High cost link. Transmission of management data (e.g. log files uploads, automatic software downloads, etc.) is limited, with most of the data being held until a low cost link is active. (Note: If required, you can allow Auto software updates and firmware updates over high cost links, by setting appropriate options. See Table G-8, General > Auto Software Updates screen fields, on page 248 for details.) <i>Note: During initial testing, avoid enabling this feature to ensure all management events are emitted. If data plan costs are a concern, enable this after the MG90 is put into operation.</i> - Not selected — Not a high cost link. <i>Note: Land mobile radio network (serial modem) links are typically very high cost and low bandwidth, while Ethernet links are typically not high cost.</i>
Change Default MTU Size	Use a different MTU Size than the default (1500 bytes). - Selected — MTU Size field can be edited. (Default) Deselect this checkbox to reset the MTU Size to the default value (the value resets when you click Save). - Not selected — MTU Size field cannot be edited. <i>Note: This may be required to accommodate some network configurations. Only change if instructed to by Sierra Wireless.</i>
MTU Size	Maximum Transmission Unit size (in bytes) - Valid range: 256–1500 - Default: 1500
Auto Local IP	Enable DHCP for this interface. - Selected — Enabled. The IP address will be assigned by a DHCP server connected to the access point network. (For most applications, the IP addresses should be obtained automatically from the network.) - Not selected — Not enabled. Assign the Local IP Address manually.
Local IP Address	Statically-assigned Local IP Address IPv4 address format (e.g. xxx.xxx.xxx.xxx) <i>Note: This field is available only if Auto Local IP is not selected.</i>
Masquerade	Network Address Translation for LAN-originated traffic leaving MG90 WAN interface - Selected — Enabled. This is the typical setting, since many carriers will disconnect a cellular modem that emits IP datagrams bearing an address other than that of the cellular modem. - Not selected — Disabled
Masquerade Port Range	Port range to use for masquerade (NAT) - Automatic — Enabled - Manual — Disabled (Default). This should be used in most cases to avoid using defined or reserved ports. <i>Note: This field is available only if Masquerade is selected.</i>

Table E-5: WAN > Links > Configure (Serial (modem)) screen fields (Continued)

Field	Description
Minimum Port Number	Range of ports to use for masquerade (NAT)
Maximum Port Number	- Default range: 49152–65535 - Valid range: 0–65535 - If Minimum Port Number < 49152: - traffic on ports lower than 512 is mapped to other ports lower than 512 - traffic on ports 512 to 1024 is mapped to ports lower than 1024 - traffic on ports greater than 1024 is mapped to ports greater than 1024 <i>Note: This field is available only if Masquerade is selected and Masquerade Port Range is Manual.</i>
Automatic DNS	DNS servers to be used - Selected — Use DNS servers specified by DHCP server. - Not selected — Use the DNS servers specified in Primary DNS or Secondary DNS. The fastest-responding server (regardless of whether named as Primary or Secondary) is chosen as the server to use. Periodically, the servers are re-evaluated to make sure the fastest-responding server is being used. If private DNS servers are used, set up DNS zones — see Configuring DNS Zones for Private DNS Server Use on page 82 for details. <i>Note: This must be disabled (not selected) if using a static IP address.</i>
Primary DNS	IP address of primary domain name server - Format: IPv4 address (xxx.xxx.xxx.xxx) - Required field (when Automatic DNS is not selected) <i>Note: This field is available only if Automatic DNS is not selected.</i>
Secondary DNS Servers	IP addresses of secondary domain name servers - Format: IPv4 addresses, comma-separated (e.g. xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy) - Optional field <i>Note: This field is available only if Automatic DNS is not selected.</i>
Auto Remote IP	Enable DHCP for this interface. - Selected — Enabled. The IP address will be assigned by a DHCP server connected to the access point network. (For most applications, the IP addresses should be obtained automatically from the network.) - Not selected — Not enabled. Assign the Local IP Address manually.
Remote IP Address	Statically-assigned Remote IP Address IPv4 address format (e.g. xxx.xxx.xxx.xxx) <i>Note: This field is available only if Auto Remote IP is not selected.</i>
Serial Modem Speed (bauds)	Serial modem baud rate Select the speed of the connected serial modem device: 9600 19200 38400 57600 115200

Table E-5: WAN > Links > Configure (Serial (modem)) screen fields (Continued)

Field	Description
Modem Initialization	AT command sequence for initializing modem For specific settings, see source.sierrawireless.com or contact your mobile network operator.
Dial String	Dial string to connect to mobile network operator's network
Use Management Tunnel	Management Tunnel usage The management tunnel is a dedicated secure VPN connection between the MG90 and AMM. - Selected — AMM can access the MG90. (Default) - Not selected — Do not use the management tunnel. AMM cannot access the MG90. To configure the management tunnel, see WAN > VPNs > (Management Tunnel) > Configure on page 202.
Monitors	Monitor(s) being used to monitor the link's connection Select one or more monitors. Factory-defined monitor — DefaultMonitor. This example should be replaced with your own monitor definition. To configure monitors, see WAN > Monitors > Configure on page 200.
Monitor Mode	Effect of selected monitors' state on link status - Success in one monitor keeps the link up — If at least one monitor is reporting as active, then the link should be considered 'up'. - Failure in one monitor declares the link down — If any one monitor is reporting as inactive, then the link should be considered 'down'. <i>Note: This field is meaningful only if one or more monitors are selected.</i>
Call Down Recovery	Reboot the router if link is down for too long When this option is enabled, the serial modem will reboot when the link goes down for longer than the Recovery Interval period. - Selected — Enabled - Not selected — Disabled (Default)
Recovery Time (seconds)	Maximum link recovery period If the link goes down for longer than this period (in seconds), the serial modem will reboot. - Default: 600 - Minimum: 1 <i>Note: This field is available only if Call Down Recovery is selected.</i>
VPN	VPNs that the WAN link can establish when the link is active If multiple VPNs are selected, each of the VPNs must be LAN to LAN. To configure VPNs, see WAN > VPNs on page 201. Warning: In the VPN field, if a VPN profile is selected that is configured as a full tunnel (subnet 0.0.0.0/0), do not select any other profiles. If the full tunnel profile and another profile are selected, none of the changes made to the screen will be saved when Save is clicked.

Table E-5: WAN > Links > Configure (Serial (modem)) screen fields (Continued)

Field	Description
Connection Method	Number of VPN tunnels to establish for a WAN connection - Connect One — Only 1 tunnel established for the WAN link, using selected method below: - Random — Establish tunnel on a randomly selected VPN from the VPN list. If tunnel cannot be established or fails, use next randomly selected VPN. This results in basic (unmanaged) load balancing across VPN servers. - Round Robin - Alphanumeric Order — Establish tunnel on the first VPN (sorted by name) in the VPN list. If tunnel cannot be established or fails, use next VPN (in sorted order). This is a redundant failover method that does not have any load-balancing characteristics. - Connect All — Tunnels to all VPNs in the VPN list established simultaneously for the WAN link. <i>Note:</i> This option (Connect All) can only be selected for LAN-to-LAN VPNs. <i>Note:</i> Any changes to Connection Method take effect after the next reboot.
Enable Custom txqueuelen	Allow customized transmission buffer size When enabled, the specified number of packets (txqueuelen value) will be held in the transmit buffer of the WAN interface. This helps to prevent packets from being dropped on slower WAN connections. - Selected — Enabled. Set the buffer size to the txqueuelen value (next field). - Not selected — Disabled (Default). Use the default txqueuelen value. <i>Note:</i> This field should not be changed without assistance from Sierra Wireless.
txqueuelen value	Customized transmission buffer size Default: 10 <i>Note:</i> This field is available only if Enable Custom txqueuelen is selected.

E.1.2 WAN Link Policy Configuration (WAN> Links > Policies)

The WAN Link Policy Configuration screen displays the policy types that are available for the selected WAN link type.

The example in [Figure E-7](#) shows the policies available for Cellular devices. Other device types will show some or all of these policies.

For details on setting up policies, see [Setting up WAN Link Policies](#) on page 51.

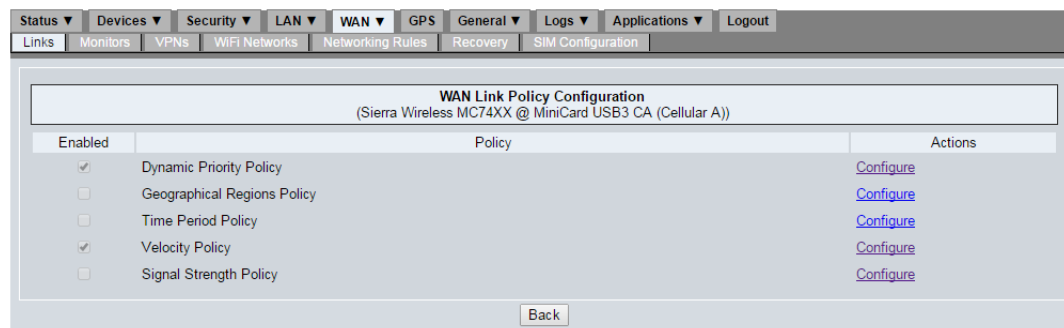


Figure E-7: LCI: WAN > Links > Policies—Sample screen

Table E-6: WAN > Links > Policies screen fields

Field	Description
Enabled	Indicates whether the associated policy is currently enabled for the WAN link. - Selected — Policy is enabled for the WAN link. - Not selected — Policy is not enabled. To enable/disable a policy, click Configure.
Policy	Policy types that can be enabled for the WAN link (available policy types vary by WAN link type): - Dynamic Priority Policy — See Dynamic Priority Policy on page 191 for details. - Geographical Regions Policy — See Geographical Regions Policy on page 192 for details. - Time Period Policy — See Time Period Policy on page 193 for details. - Velocity Policy — See Velocity Policy on page 194 for details. - Signal Strength Policy — See Signal Strength Policy on page 195 for details.
Actions	The only available action type for policies is Configure. Configure — Click to configure link-specific policy details

E.1.2.1 WAN > Links > Policies > Configure

Dynamic Priority Policy

The Dynamic Priority Policy Configuration allows you to assign a base score adjustment, and to assign an adjustment that dynamically changes based on the solidity of the connection.

See [Dynamic Priority Policy Overview](#) on page 53 for details.

The screenshot shows the 'WAN Link Priority Policy Configuration' window. At the top, there's a title bar with tabs: Status, Devices, Security, LAN, WAN (selected), GPS, General, Logs, Applications, and Logout. Below the tabs are sub-tabs: Links, Monitors, VPNs, WiFi Networks, Networking Rules (selected), Recovery, and SIM Configuration. The main content area is titled 'WAN Link Priority Policy Configuration (Sierra Wireless MC74XX @ MiniCard USB3 CA (Cellular A))'. It contains several settings: 'Enable this policy' with a checked checkbox, 'Priority Score' with a text box containing '1800' and a lock icon, 'Enable Dynamic Priority' with a checked checkbox, 'Link Down Penalty' with a text box containing '300', and 'Recovery Period (Seconds)' with a text box containing '120'. At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure E-8: LCI: WAN > Links > Policies > Configure (Dynamic) — Sample screen

Table E-7: WAN > Links > Policies > Configure (Dynamic) screen fields

Field	Description
Enable this policy	Enable/disable the policy for the WAN link. - Selected — Enabled - Not selected — Disabled. If you disable a policy after configuring it, the configuration settings do not reset to default values, so they can still be used if you re-enable the policy.

Table E-7: WAN > Links > Policies > Configure (Dynamic) screen fields (Continued)

Field	Description
Priority Score	Base priority score adjustment (value to add to the base score) All links start with a base score of 1000. Use this field to adjust this link's base score. (The link with the highest score will be the active link when multiple links are available.) For example, if this field is 100, the link's adjusted base score before applying any other policy adjustments is 1100 (1000 + 100).
Enable Dynamic Priority	Enable / disable dynamic priority score recovery When a down link is restored, a dynamic priority policy will determine the next suitable active link over a period of time to avoid unnecessary switching caused by instability of the recovered link. This is accomplished by gradually incrementing the recovered link's score over the recovery period. - Selected — Enabled. Use the Link Down Penalty and Recovery Period to gradually restore the link's base priority score. - Not selected — Disabled. When a down link is restored, its priority score is immediately set to its normal value.
Link Down Penalty	Priority score reduction applied to 'down' link When a down link recovers, this value is immediately subtracted from its base priority score. This penalty is removed linearly over the specified Recovery Period. Examples: - Penalty=60, Recovery Period= 120 seconds When the down link first recovers, apply this penalty then begin decreasing it by 0.5 points / second. - Penalty=240, Recovery Period = 120 seconds When the down link first recovers, apply this penalty then begin decreasing it by 2 points / second. <i>Note: This field applies only if Enable Dynamic Priority is selected.</i>
Recovery Period (seconds)	Link Down Penalty recovery period Period of time, in seconds, over which the Link Down Penalty decreases until it is completely removed. - Default: 0 - Recommended range: 0–600 <i>Note: If the link disconnects again during the recovery period, the Link Down Penalty and Recovery Period are re-applied when the link comes back online.</i> <i>Note: This field applies only if Enable Dynamic Priority is selected.</i>

Geographical Regions Policy

Use the geographical regions policy to consider the vehicle's location when determining which network to use. Up to three regions can be defined. When the vehicle travels into a defined region, an adjustment is applied to the link's score.

Each region is a rectangular area defined by:

- Upper-left latitude and longitude
- Lower-right latitude and longitude

See [Geographical Regions Policy Overview](#) on page 55 for details.

WAN Link Geographical Region Policy Configuration
(Sierra Wireless MC74XX@ MiniCard USB3 CA (Cellular A))

Enable all region policies ☒

Region 1		Region 2		Region 3	
Upper Left Latitude	49.2858	Upper Left Latitude	49.2800	Upper Left Latitude	0.0
Upper Left Longitude	-123.1286	Upper Left Longitude	-123.0845	Upper Left Longitude	0.0
Lower Right Latitude	49.2764	Lower Right Latitude	49.0001	Lower Right Latitude	0.0
Lower Right Longitude	-123.0773	Lower Right Longitude	-123.0612	Lower Right Longitude	0.0
Score	200	Score	100	Score	0

Save Cancel

Figure E-9: LCI: WAN > Links > Policies > Configure (Geographical)—Sample screen

Table E-8: WAN > Links > Policies > Configure (Geographical) screen fields

Field	Description
Enable all region policies	Enable/disable the geographical region policies for the WAN link - Selected—Enabled. All three region policies are used. To use only one or two policies, set the latitude and longitude values for the unused regions to 0.0. - Not selected—Disabled. None of the region policies are used. Note: If you disable the policies after configuring them, the configuration settings do not reset to default values, so they can still be used if you re-enable the policies.
Upper Left Latitude	Latitude/longitude coordinates of rectangular region - Format: Decimal (decimal portion rounds to four places) - Example: - Upper Left Latitude: 49.2858 (49° 17' 08" N) - Upper Left Longitude: -123.1286 (123° 07' 42" W) - Lower Right Latitude: 49.2764 (49° 16' 35" N) - Lower Right Longitude: -123.0773 (123° 04' 38" W)
Upper Left Longitude	
Lower Right Latitude	
Lower Right Longitude	
Score	Score adjustment value The value that will be added to the link's score for determining network selection.

Time Period Policy

Use the time period policy to consider the time of day when determining which network to use. Up to three time periods can be defined. Each period score is added to determine the network selection when the current time falls within the period.

Important: Ensure the time periods do not overlap.

See [Time Period Policy Overview](#) on page 57 for details.

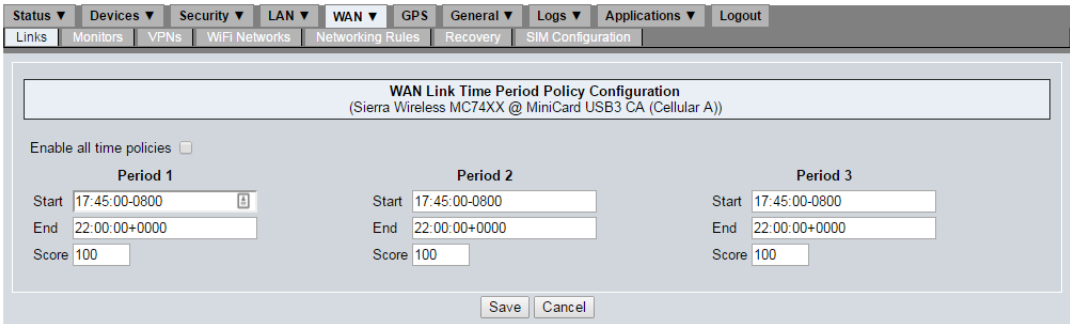


Figure E-10: LCI: WAN > Links > Policies > Configure (Time Period)—Sample screen

Table E-9: WAN > Links > Policies > Configure (Time Period) screen fields

Field	Description
Enable all time policies	Enable/disable the time period policies for the WAN link - Selected—Enabled. All three time period policies are used. To use only one or two policies, set the start and end values for the unused periods to 00:00:00+0000. - Not selected—Disabled. None of the time period policies are used. <i>Note: If you disable the policies after configuring them, the configuration settings do not reset to default values, so they can still be used if you re-enable the policies.</i>
Start	Starting and ending times for the period - Format: HH:mm:ss±hhmm (where hhmm is the offset from UTC) - For example, the following values all represent the same time: 10:15:00+0000 14:15:00+0400 06:45:00-0330
End	
Score	Score adjustment value The value that will be added to the link's score for determining network selection.

Velocity Policy

Use the velocity policy to allow for proactive network switching based on vehicle velocity instead of relying only on network outage switching. For example, you may prefer to give Wi-Fi a preference while stationary (e.g. in a depot) and cellular a preference while moving.

See [Velocity Policy Overview](#) on page 57 for details.

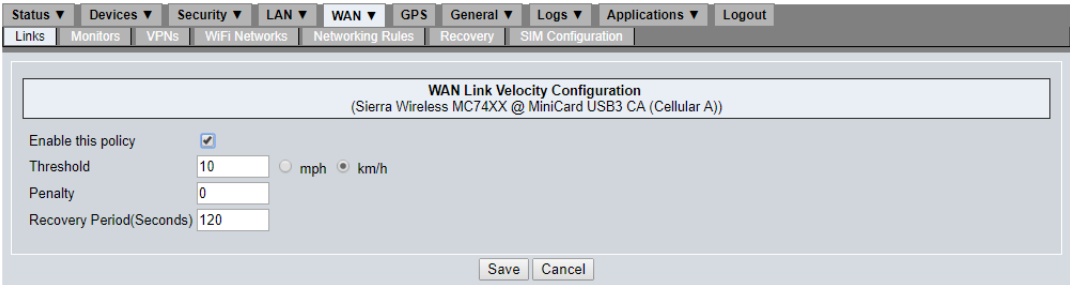


Figure E-11: LCI: WAN > Links > Policies > Configure (Velocity)—Sample screen

Table E-10: WAN > Links > Policies > Configure (Velocity) screen fields

Field	Description
Enable this policy	Enable / disable the policy for the WAN link: - Selected — Enabled. - Not selected — Disabled. <i>Note: If you disable the policy after configuring it, the configuration settings do not reset to default values, so they can still be used if you re-enable the policy.</i>
Threshold	Maximum velocity before Penalty is applied If the vehicle's velocity exceeds this value, the Penalty is applied to the link's score. Select the appropriate velocity unit (mph or km/h) for the threshold value that you entered.
Penalty	Score adjustment value This value is immediately subtracted from the link's score when the velocity exceeds the threshold. When the velocity decreases below the threshold, the penalty is removed linearly over the specified Recovery Period. Examples: - Penalty=60, Recovery Period=120 seconds When velocity decreases below the threshold, the penalty begins to decrease by 0.5 points / second. - Penalty=240, Recovery Period =120 seconds When velocity decreases below the threshold, the penalty begins to decrease by 2 points / second.
Recovery Period (Seconds)	Period of time (in seconds) the vehicle's velocity must remain below the Threshold before the Penalty is completely removed Default: 120 (2 minutes) <i>Note: If the velocity exceeds the threshold during the recovery period, the Penalty and Recovery Period are re-applied</i>

Signal Strength Policy

Use the signal strength policy to allow for proactive network switching based on the WAN connection's RF condition, indicated by a selection of metrics (RSSI, RSRP, RSRQ, SINR) instead of relying only on network outage switching.

See [Signal Strength Policy Overview](#) on page 58 for details.

Note: Metric thresholds do not reset to defaults when disabled and re-enabled.

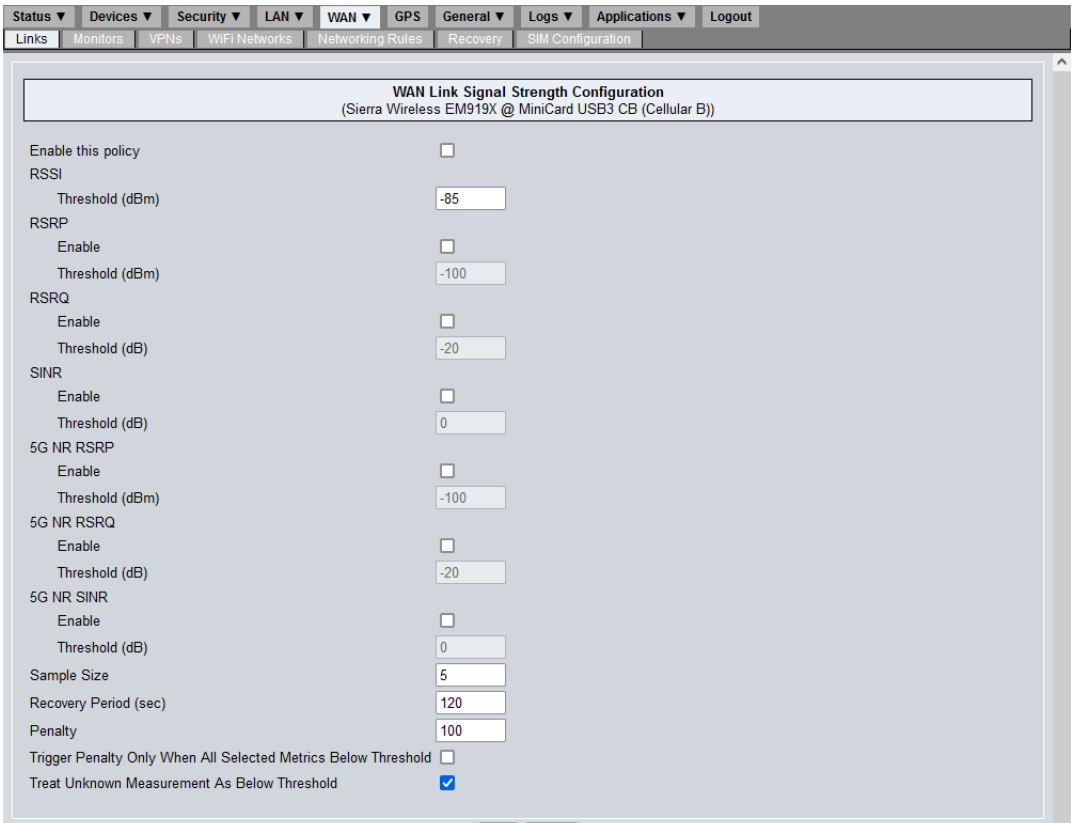


Figure E-12: LCI: WAN > Links > Policies > Configure (Signal Strength)—Sample screen

Table E-11: WAN > Links > Policies > Configure (Signal Strength) screen fields

Field	Description
Enable this policy	Enable/disable the policy for the WAN link: - Selected — Enabled. - Not selected — Disabled. <i>Note: This option applies to the entire policy. The other 'Enable' fields on this screen apply only to their respective metrics. i.e., If the policy is enabled and all other Enable fields are not selected, the policy will consider only the RSSI metric.</i>
RSSI	
Threshold (dBm)	If the RSSI is lower than this value, apply the Penalty to the link's score (depending on the Trigger Penalty Only When All Selected Metrics Below Threshold setting). Default: -85 dBm <i>Note: The default threshold of -85 dBm is typically sufficient to drop bad connections that may not cause ping monitor failures, while also ensuring the MG90 does not unnecessarily switch to a lower throughput link that has a stronger signal.</i>

Table E-11: WAN > Links > Policies > Configure (Signal Strength) screen fields (Continued)

Field	Description
RSRP	
Enable	Include LTE RSRP (Reference Signal Received Power) when evaluating the Signal Strength policy - Selected — Include - Not selected — Do not include
Threshold (dBm)	LTE RSRP If the LTE RSRP is lower than this value, apply the Penalty to the link's score (depending on the Trigger Penalty Only When All Selected Metrics Below Threshold setting). Default: -100 dBm <i>Note: The default threshold of -100 dBm is typically sufficient to drop bad connections that may not cause ping monitor failures, while also ensuring the MG90 does not unnecessarily switch to a lower throughput link that has a stronger signal.</i>
RSRQ	
Enable	Include LTE RSRQ (Reference Signal Received Quality) when evaluating the Signal Strength policy - Selected — Include - Not selected — Do not include
Threshold (dB)	LTE RSRQ If the LTE RSRQ is lower than this value, apply the Penalty to the link's score (depending on the Trigger Penalty Only When All Selected Metrics Below Threshold setting). Default: -20 dB <i>Note: The default threshold of -20 dB is typically sufficient to drop bad connections that may not cause ping monitor failures, while also ensuring the MG90 does not unnecessarily switch to a lower throughput link that has a stronger signal.</i>
SINR	
Enable	Include LTE SINR (Signal to Interference and Noise Ratio) when evaluating the Signal Strength policy - Selected — Include - Not selected — Do not include
Threshold (dB)	LTE SINR If the LTE SINR is lower than this value, apply the Penalty to the link's score (depending on the Trigger Penalty Only When All Selected Metrics Below Threshold setting). Default: 0 dB <i>Note: The default threshold of 0 dB is typically sufficient to drop bad connections that may not cause ping monitor failures, while also ensuring the MG90 does not unnecessarily switch to a lower throughput link that has a stronger signal.</i>
5G NR RSRP	
Enable	Include 5G NR RSRP (Reference Signal Received Power) when evaluating the Signal Strength policy - Selected — Include - Not selected — Do not include <i>Note: This field appears only for EM9190 links.</i>

Table E-11: WAN > Links > Policies > Configure (Signal Strength) screen fields (Continued)

Field	Description
Threshold (dBm)	5G NR RSRP If the 5G NR RSRP is lower than this value, apply the Penalty to the link's score (depending on the Trigger Penalty Only When All Selected Metrics Below Threshold setting). Default: -100 dBm <i>Note: The default threshold of -100 dBm is typically sufficient to drop bad connections that may not cause ping monitor failures, while also ensuring the MG90 does not unnecessarily switch to a lower throughput link that has a stronger signal.</i> <i>Note: This field appears only for EM9190 links.</i>
5G NR RSRQ	
Enable	Include 5G NR RSRQ (Reference Signal Received Quality) when evaluating the Signal Strength policy - Selected — Include - Not selected — Do not include <i>Note: This field appears only for EM9190 links.</i>
Threshold (dB)	5G NR RSRQ If the 5G NR RSRQ is lower than this value, apply the Penalty to the link's score (depending on the Trigger Penalty Only When All Selected Metrics Below Threshold setting). Default: -20 dB <i>Note: The default threshold of -20 dB is typically sufficient to drop bad connections that may not cause ping monitor failures, while also ensuring the MG90 does not unnecessarily switch to a lower throughput link that has a stronger signal.</i> <i>Note: This field appears only for EM9190 links.</i>
5G NR SINR	
Enable	Include 5G NR SINR (Signal to Interference and Noise Ratio) when evaluating the Signal Strength policy - Selected — Include - Not selected — Do not include <i>Note: This field appears only for EM9190 links.</i>
Threshold (dB)	5G NR SINR If the 5G NR SINR is lower than this value, apply the Penalty to the link's score (depending on the Trigger Penalty Only When All Selected Metrics Below Threshold setting). Default: 0 dB <i>Note: The default threshold of 0 dB is typically sufficient to drop bad connections that may not cause ping monitor failures, while also ensuring the MG90 does not unnecessarily switch to a lower throughput link that has a stronger signal.</i> <i>Note: This field appears only for EM9190 links.</i>

Table E-11: WAN > Links > Policies > Configure (Signal Strength) screen fields (Continued)

Field	Description
Sample Size	Number of samples to include when evaluating policy Samples of all enabled metrics are collected every 2 seconds and the policy is evaluated using the average values for each sampled metric (for this number of samples). - Default: 5 For example, samples A, B, C, D, E, F, G, H, I, J are taken 2 seconds apart. - When sample E is taken, the policy is evaluated with samples A, B, C, D, E. - When sample F is taken, the policy is evaluated with samples B, C, D, E, F. - When sample G is taken, the policy is evaluated with samples C, D, E, F, G. - etc.
Recovery Period (sec)	Period of time (in seconds) that the metrics that caused the penalty must remain above their respective thresholds before the penalty is removed. Default: 120 (2 minutes) Note: If any or all sampled metrics drop below their respective thresholds during the recovery period (depending on the Trigger Penalty Only When All Selected Metrics Below Threshold setting), the Penalty remains in effect and the Recovery Period restarts.
Penalty	Score adjustment value This value is immediately subtracted from the link's score when any or all sampled metrics falls below their respective thresholds (depending on the Trigger Penalty Only When All Selected Metrics Below Threshold setting). When the metric(s) increase and remain above their thresholds for the entire Recovery Period, the penalty is removed.
Trigger Penalty Only When All Selected Metrics Below Threshold	When to apply the Penalty to the link's score - Selected — The Penalty is applied only when all 'enabled' metrics are below their respective thresholds. (i.e., every selected metric is 'bad') - Not selected — The Penalty is applied when any 'enabled' metric is below its respective threshold. (i.e., any indication of a 'bad' signal triggers the penalty)
Treat Unknown Measurement As Below Threshold	What to do if an enabled metric is not collected in the sample - Selected — Assume the metric is below threshold (i.e., indicates a 'bad' signal) - Not selected — Assume the metric is above the threshold

E.2 WAN > Monitors

The Monitors tab is used to create and configure monitors to detect and recover from high-level communication failures.

Note: A 'DefaultMonitor' is provided. Each time you add a new monitor, it uses the same initial default settings (so if you delete the DefaultMonitor by accident, you can simply use Add New WAN Monitor to recreate it).

See [Using WAN Monitors to Detect Lost Connections](#) on page 49 for details.

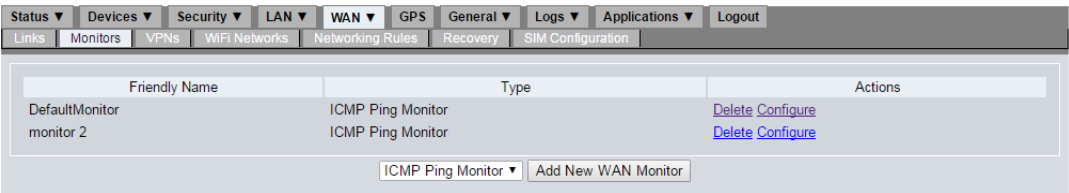


Figure E-13: LCI: WAN > Monitors—Sample screen

Table E-12: WAN > Monitors screen fields

Field	Description
Friendly Name	Descriptive name for the monitor
Type	Monitor type (cannot be modified). Always appears as “ICMP Ping Monitor”.
Actions	Click these optional links to perform actions on the associated monitors: - Delete — Delete the associated monitor. <i>Caution: The monitor deletes immediately, even if it is in use by any of the WAN links. If you delete the monitor by mistake, you will have to recreate it and then enable it in each of the affected WAN links.</i> - Configure — Configure monitor-specific details. See WAN > Monitors > Configure on page 200.
Add new WAN Monitor (button)	Click to display the configuration screen, using default values for all fields. The new monitor is added when you click Save after editing the configuration fields. See WAN > Monitors > Configure on page 200.

E.2.1 WAN > Monitors > Configure

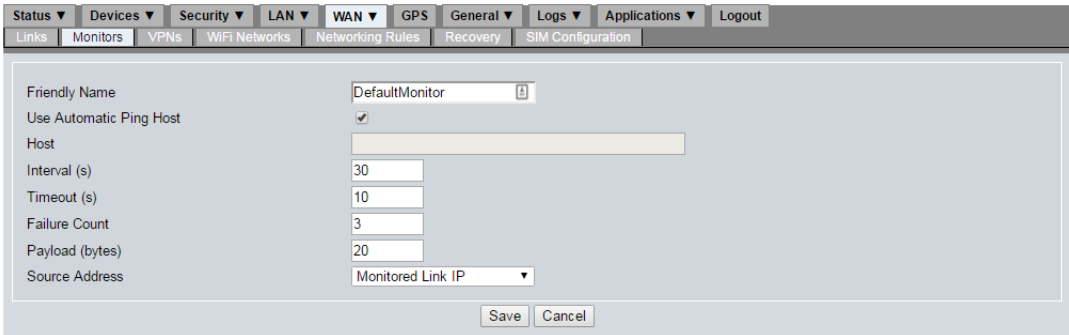


Figure E-14: LCI: WAN > Monitors > Configure (or Add)—Sample screen

Table E-13: WAN > Monitors > Configure (or Add) screen fields

Field	Description
Friendly Name	Descriptive name for the monitor This is the name that identifies the monitor on the WAN Link Configuration pages.

Table E-13: WAN > Monitors > Configure (or Add) screen fields (Continued)

Field	Description
Use Automatic Ping Host	Use the default ping host, or specify a different host - Selected — Send pings to <ESN>.ping.omgservice.com (where <ESN> is the MG90's serial number, shown in the title bar of the LCI, and in Status > General). (Note — If you select this option and save the monitor, the Host field is cleared.) - Not selected — Specify a ping host in the Host field.
Host	IP address or URL of the host to ping. IPv4 address format (e.g. xxx.xxx.xxx.xxx) <i>Note: This field applies only if Use Automatic Ping Host is not selected.</i>
Interval (s)	Ping interval Ping the host to confirm the link is active. Wait this number of seconds between sending each ping. Default: 30
Timeout (s)	Ping response timeout Number of seconds to wait for a response to a ping. If a response is not received, increase the number of consecutive ping failures. Default: 10
Failure Count	Maximum allowed consecutive ping failures If this number of consecutive pings fail, restart the WAN link. Default: 3
Payload (bytes)	Ping packet size Number of bytes sent in a single ping request. Default: 20
Source Address	VPN source address Select a different source address when configuring the VPN Ping Monitor. This will be populated with the LAN segments available, along with the Link IP. For the ICMP datagram to be allowed through the VPN, it <i>must</i> have the source address used to specify the VPN connection.

E.3 WAN > VPNs

The VPNs tab is used to create and configure VPN profiles that allow access to Virtual Private Networks (VPNs).

See [How to configure a VPN](#) on page 77 for details.

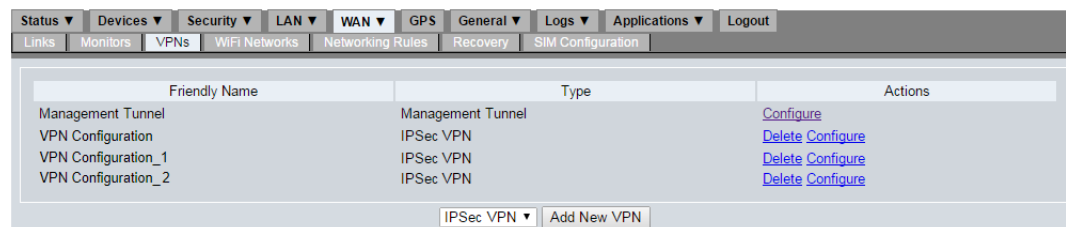


Figure E-15: LCI: WAN > VPNs—Sample screen

Table E-14: WAN > VPNs screen fields

Field	Description
Friendly Name	Descriptive name for the VPN, defined in the Configure screen.
Type	VPN type - Management Tunnel — Dedicated secure VPN connection between the MG90 and AMM. - IPSec VPN — User-defined VPN
Actions	Click these optional links to perform actions on the associated VPN profiles: - Delete — Delete the associated VPN. (Note — This option is not available for the Management Tunnel.) <i>Caution:</i> The VPN is deleted immediately, even if it is in use by any of the WAN links. If you delete the VPN by mistake, you will have to recreate it and then enable it in each of the affected WAN links. - Configure — Configure VPN-specific details. See IPSec VPN Configuration (WAN > VPNs > Add New VPN, and WAN > VPNs > (IPSec VPN) > Configure) on page 204.
Add New VPN (button)	Click to display the configuration screen, using default values for all fields. The new VPN is added when you click Save after editing the configuration fields. <i>Note:</i> The drop-down includes one option only—IPsec VPN.

E.3.1 WAN > VPNs > (Management Tunnel) > Configure

The management tunnel is a dedicated secure VPN connection between the MG90 and AMM. It provides secure remote console access, remote LCI, mass configuration, and event notification.

The screenshot shows the 'Management Tunnel VPN Configuration' screen. It has a navigation bar at the top with tabs: Status, Devices, Security, LAN, WAN (selected), GPS, General, Logs, Applications, and Logout. Below the navigation bar are sub-tabs: Links, Monitors, VPNs (selected), WiFi Networks, Networking Rules, Recovery, and SIM Configuration. The main content area contains the following fields:

- Automatic Gateway Manager 1: ☒
- Gateway Manager 1:
- Automatic Gateway Manager 2: ☒
- Gateway Manager 2:
- Available UDP Ports: ☒ 1194 ☒ 1195 ☒ 1196 ☒ 1197
- Enable Tunnel Automatic Monitor: ☒

At the bottom of the form are 'Save' and 'Cancel' buttons.

Figure E-16: LCI: WAN > VPNs > Configure—Sample screen

Table E-15: WAN > VPNs > (Management Tunnel) > Configure screen fields

Field	Description
Automatic Gateway Manager 1	Use first default gateway manager (<ESN>.dels.omgservice.com, where <ESN> is the MG90's serial number)
Gateway Manager 1	Gateway Manager IPv4 address or FQDN of your first private AMM server <i>Note:</i> This field applies only if Automatic Gateway Manager 1 is not selected.
Automatic Gateway Manager 2	Use second default gateway manager (<ESN>.dels.omgservice.com, where <ESN> is the MG90's serial number)

Table E-15: WAN > VPNs > (Management Tunnel) > Configure screen fields (Continued)

Field	Description
Gateway Manager 2	Gateway Manager IPv4 address or FQDN of your second private AMM server <i>Note: This field applies only if Automatic Gateway Manager 2 is not selected.</i>
Available UDP Ports	UDP Ports for Management Tunnel Select the UDP port(s) that the management tunnel can be brought up on. If more than one port is selected, the management tunnel will be brought up on one of the ports randomly. <i>Note: If AMM 2.15 or earlier is being used, select UDP port 1194.</i>
Enable Tunnel Automatic Monitor	Enable/disable Management Tunnel Monitor - Selected — Enabled. A ping monitor is enabled which will periodically ping AMM to test for connectivity. - Not selected — Disabled.

E.3.2 IPSec VPN Configuration (WAN > VPNs > Add New VPN, and WAN > VPNs > (IPSec VPN) > Configure)

The IPSec VPN Configuration screen is used to add or update VPN profiles.

The screenshot shows the 'IPsec VPN Configuration' screen. The top navigation bar includes tabs for Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below this is a sub-navigation bar with links for Links, Monitors, VPNs, WiFi Networks, Networking Rules, Recovery, and SIM Configuration. The main configuration area is titled 'IPsec VPN Configuration' and contains the following fields:

- Friendly Name: VPN Configuration
- Server Address: [Empty]
- Server ID: [Empty]
- Remote Network: 10.0.1.0/24 (Comma separated CIDR notation)
- Allow Management Tunnel Bypass: [Checked]
- IPsec Address Exemptions: [Empty] (Comma separated IP or hostname)
- Local Termination: Network
- Local Subnets: Default LAN - 172.22.0.0/24, Serial LAN - 172.22.1.0/24
- Gateway Virtual IP: Automatic (IKEv2 Only), Manual
- Internet Key Exchange: IKEv2
- IKE Transform: aes128-md5 dh-group 5
- MOBIKE: [Checked]
- Single Subnet Per Child SA: [Checked]
- Dead Peer Detection: [Checked]
- Delay (sec): 10
- Timeout (sec): 30
- IKE Lifetime (min): 60
- Reauthenticate on IKE ReKey: [Checked]
- IPsec: negotiated (not including dh-group)
- IP Compression: [Unchecked]
- Force UDP Encapsulation: [Checked]
- Authentication: Certificate
- Auth ID: ESN, ND60510040011018
- CA Certificate File: Choose File, No file chosen
- Certificate Profile: default
- Server Certificate File: Choose File, No file chosen
- Monitors: DefaultMonitor

At the bottom of the screen are 'Save' and 'Cancel' buttons.

Figure E-17: LCI: WAN > VPNs > Add New VPN—Sample screen

Table E-16: WAN > VPNs > Add New VPN (or Configure) screen fields

Field	Description
Friendly Name	Enter a descriptive nickname for the VPN. This name identifies the VPN in other LCI screens (e.g. WAN > Links > Configure).
Server Address	Enter the VPN Gateway IP Address (IP address or FQDN) - IPv4 address format (e.g. xxx.xxx.xxx.xxx) - FQDN format (e.g. test.mycompany.net)

Table E-16: WAN > VPNs > Add New VPN (or Configure) screen fields (Continued)

Field	Description
Server ID	The ID that the VPN server uses to identify itself to the router while negotiating the VPN tunnel. The ID format depends on the selected Authentication Method: ▪ Password authentication — IP address, FQDN, hostname, or domain name ▪ Certificate authentication — VPN server's certificate "Subject" The ID should be provided by the VPN server administrator. Examples: ▪ Password authentication: • (IP address) Blank — Use the Server Address • (IP address) 192.168.45.3 • (Hostname) Test1 • (FQDN) test.yourcompany.net ▪ Certificate authentication: • (VPN server side certificate Subject field) — Example: "C=CA, ST=BC, O=companyname, OU=QA, CN=testtest, emailAddress=response@inmotiontechnology.com" <i>Note: If the Subject field includes any slash (/) characters, replace them with commas (,).</i>
Remote Network	
Remote Subnets	Destination IP network and destination IP network mask in CIDR notation. ▪ IPv4 CIDR address format addresses, comma-separated (e.g. xxx.xxx.xxx.xxx/yy) ▪ Example: 192.168.254.0/24
Allow Management Tunnel Bypass	Management Tunnel usage The management tunnel is a dedicated secure VPN connection between the MG90 and AMM. AMM always uses the management tunnel to communicate with the MG90. ▪ Selected — Use this option if AMM has a public IP address. (i.e., AMM is routable outside the IPsec VPN — it does not have a private IP address (10.x.x.x, 172.x.x.x, 192.x.x.x)) (Default) ▪ Not selected — Use this option if AMM is inside the IPsec VPN. (e.g., if the IPsec VPN subnet is 10.0.1.0/24 and the AMM address is 10.0.1.3) To configure the management tunnel, see WAN > VPNs > (Management Tunnel) > Configure on page 202.
IPsec Address Exemptions	Traffic generated on the MG90 to the IP addresses (or Fully Qualified Domain Names (FQDNs)) in this list is sent directly to the Internet (i.e., the traffic is not sent through the IPsec VPN tunnel). ▪ IPv4 addresses and /or FQDNs, comma-separated
Local Termination	Local termination type ▪ Host — Host to LAN configuration ▪ Network — LAN to LAN configuration (Network terminated) <i>Important: All VPN profiles should use the same Local Termination type (all should be Host-to-LAN, or all should be LAN-to-LAN), even if they are not selected for use in any of the WAN link configurations.</i>
Local Subnets	Local subnets (LAN Segments) Select the LAN segments to use for this VPN. <i>Note: LAN segments are configured in LAN > LAN Segments.</i>

Table E-16: WAN > VPNs > Add New VPN (or Configure) screen fields (Continued)

Field	Description
Gateway Virtual IP	IP address of the gateway (VPN peer) - Automatic — Receive virtual IP address dynamically from the VPN server. - Manual — Manually assign the virtual IP address based on the Local Termination type: - Host — Use the gateway virtual IP address (i.e. a host address to use for the VPN, not an IP address on the LAN segment) - Network — IP address that the MG90 has on one of the selected LAN segments (Local Subnets) selected on the VPN. - IPv4 address format (e.g. xxx.xxx.xxx.xxx) Note: This field is not used for IKEv1. This feature is supported only when Internet Key Exchange (IKE) V2 is used. Multiple VPN is not supported if any of the VPN profiles are using automatic Virtual IP addresses.
Internet Key Exchange	Select the Internet Key Exchange (IKE) protocol version used for this VPN. - IKEv1 - IKEv2 Warning: Creating a VPN profile using IKEv1 will affect the network hand-off performance of other VPN profiles using MOBIKE. This is true even when the the IKEv1 profile is not selected in any WAN link.
IKE Transform	Select the appropriate IKE transform for this VPN. Note: The list of available transforms varies depending on the selected Internet Key Exchange version. Note: The IKE Transform must be a supported configuration on the VPN server.
MOBIKE	Use the MOBIKE (IKEv2 Mobility and Multihoming) protocol - Selected — Enabled. (Note — Use this option only when using a VPN server (ACM or other appliance) that supports MOBIKE.) - Not selected — Not enabled. Note: This field is available only if the Internet Key Exchange value is IKEv2. If MOBIKE is used for any VPN, all VPNs on the system must also use the IKEv2 transform.
Single Subnet Per Child SA	Important This option should only be selected (enabled) for connection to Cisco ASA (and similar VPN servers). For all other VPN servers, leave this option unselected. Selecting this option enables the use of multiple local and / or remote LAN-to-LAN subnets or multiple remote Host-to-LAN subnets when connecting to a Cisco ASA (Adaptive Security Appliance) or similar server using IKEv2. For any other configurations, this option should not be selected. - Selected — Enable (A separate child SA is created for each remote subnet.) - Not selected — Disable (All subnets use the same child SA, per IKEv2 default settings.) Note: This option is only considered when IKEv2 is selected as the Internet Key Exchange type.
Dead Peer Detection	Enable / disable Dead Peer Detection If enabled, dead peer detection can detect when an IKE peer is unavailable. Note: Do not select this option if MOBIKE is enabled. - Selected — Enabled. Detection attempts are based on the Delay and Timeout values. - Not selected — Disabled. Note: Do not rely solely on DPD. Sierra Wireless recommends the use of VPN link monitors to ensure reliable failure detection and recovery.

Table E-16: WAN > VPNs > Add New VPN (or Configure) screen fields (Continued)

Field	Description
Delay (sec)	Number of seconds between contact attempts. Default: 10 <i>Note: This field is available only if Dead Peer Detection is selected.</i>
Timeout (sec)	Number of seconds to wait for the IKE peer to respond to a contact attempt. Default: 30 <i>Note: This field is available only if Dead Peer Detection is selected.</i>
IKE Lifetime (min)	Lifetime for IKE Security Association (SA) Number of minutes before a new SA will be negotiated. Default: 60 <i>Note: Either end may initiate the negotiation; both ends need not agree.</i>
Reauthenticate on IKE ReKey	Require re-authentication when rekeying IKE security association. - Selected — Re-authentication required - Not selected — Re-authentication not required <i>Note: This field is available only if the Internet Key Exchange value is IKEv2.</i>
IPsec	
ESP Transform	ESP Transform used for IPsec security Select the appropriate ESP transform for this VPN. To enhance security, PFS (Perfect Forward Secrecy) can be enabled. This causes unique keys to be used when generating the SAs (Security Association) between the MG90/client device and VPN server. If any one key is compromised, only that specific SA is compromised. If PFS is disabled, however, the same key is used for all SAs and if the key is compromised, all SAs using that key are compromised. PFS is enabled/disabled by choosing an appropriate ESP transform: - Enable PFS — Select a transform that includes a dh-group (e.g. "aes256-sha2_256 dh-group 2"). - Disable PFS — Select a transform that does not include a dh-group (e.g. "aes256-sha2_256"). <i>Note: The ESP Transform must be a supported configuration on the VPN server.</i>
IP Compression	Enable/disable IP packet compression - Selected — Enabled - Not selected — Disabled <i>Note: This field must be disabled if the VPN server (Server Address field) doesn't support compression.</i>
Force UDP Encapsulation	Enable/disable UDP encapsulation - Selected — Enabled (Default). This is the recommended setting. When the VPN server is behind a firewall, firewall configuration is simplified as the firewall only has to allow ports 500 (IKE) and 4500 (UDP-encapsulated ESP). - Not selected — Disabled. When this setting is used, port 50 must also be allowed for the ESP protocol to pass.

Table E-16: WAN > VPNs > Add New VPN (or Configure) screen fields (Continued)

Field	Description
Authentication	
Authentication Method	Network authentication method Select the method the VPN uses to authenticate client devices. ▪ Password — Use a pre-shared key ▪ Certificate — Use a digital certificate
Auth ID	Host authentication ID string Select an ID type and enter the ID string that will be used to identify the host. ▪ ESN — The MG90's serial number (as displayed in Status > General) ▪ ip address — IP address of the active WAN link ▪ custom — A custom string. (Note: Do not include spaces in the string.)
Change Pre-Shared Key	Select to access the next three fields. <i>Note: This field appears only when updating an existing VPN that has the Authentication Method as "Password".</i>
Previous Pre-Shared Key	Enter the current password (pre-shared key). (Note that the value is obfuscated for security reasons.) <i>Note: This field appears only when updating an existing VPN that has the Authentication Method as "Password".</i>
Pre-Shared Key or New Pre-Shared Key	Enter a new non-blank password (pre-shared key), and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.) ▪ The key cannot contain the following special characters: '\$', ' ' <i>Note: These fields are available only when the Authentication Method is "Password".</i>
Retype Pre-Shared Key or Retype New Pre-Shared Key	
Activation Date	Activation date for Auth ID and Pre-Shared Key. Select this option if using a rotating credential system, and enter the date that the Auth ID and Pre-Shared Key become the active credentials. ▪ Date format: yyyy/mm/dd hh:mm <i>Note: This field is available only when the Authentication Method is "Password".</i>
Secondary Auth ID	Host authentication secondary ID string Select an ID type and enter the ID string, or select "Unused" to not use secondary authorization. This field is used as a backup to the Auth ID field. For more information contact Sierra Wireless Support. ▪ Unused — Secondary authorization is not used ▪ ESN — The MG90's serial number (as displayed in Status > General) ▪ ip address — IP address of the active WAN link ▪ custom — A custom string. (Note: Do not include spaces in the string.)
Change Secondary Pre-Shared Key	Select to access the next three fields. <i>Note: This field appears only when updating an existing VPN that has the Authentication Method as "Password", and a secondary pre-shared key is in use.</i>

Table E-16: WAN > VPNs > Add New VPN (or Configure) screen fields (Continued)

Field	Description
Previous Secondary Pre-Shared Key	Enter the current secondary password (pre-shared key). (Note that the value is obfuscated for security reasons.) <i>Note: This field is accessible only when Change Secondary Pre-Shared Key is selected.</i>
Secondary Pre-Shared Key or New Secondary Pre-Shared Key	Enter a new non-blank password (pre-shared key), and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.) The key cannot contain the following special characters: '\$', ' '
Retype Pre-Shared Key or Retype New Pre-Shared Key	<i>Note: These fields are available only when Change Secondary Pre-Shared Key is selected.</i>
Secondary Activation Date	Activation date for Secondary Auth ID and Secondary Pre-Shared Key. Select this option if using a rotating credential system, and enter the date that the Auth ID and Pre-Shared Key become the active credentials. Date format: yyyy/mm/dd hh:mm <i>Note: This field is available only when the Authentication Method is "Password" and the Secondary Auth ID is not "Unused".</i>
CA Certificate File	Click Browse/Choose File and select the CA server certificate (.pem) file to use. <i>Important: Only one certificate file can be uploaded—the file must contain both the root and intermediate certificates. If the CSA (Certificate Signing Authority) provided separate root and intermediate certificates, combine them as described in Creating a combined CA certificate on page 92 before using Browse/Choose File.</i> <i>Note: This field is available only when the Authentication Method is "Certificate".</i>
Certificate Profile	Select a profile (which identifies a signed certificate) to use for authentication. The displayed profiles are defined in Certificate Management (Security > Certificate Management). For details, see Certificate Configuration on page 85.) <i>Important: Do not select the desired profile if it is not yet completed—for example, if the MG90 is deployed before certificates are loaded. When the certificate profile is ready (CSR generated and certificate loaded), the AMM can be used to mass-configure VPNs and/or Wi-Fi networks on multiple MG90 routers with the new certificate.</i> <i>Note: This field is available only when the Authentication Method is "Certificate".</i>
Server Certificate File	Use a server certificate file - Not Selected—Use a CA certificate server. - Selected—Select only when a CA certificate server is not available, then click Browse/Choose File to select the server certificate file to use. <i>Note: This field is available only when the Authentication Method is "Certificate".</i>

Table E-16: WAN > VPNs > Add New VPN (or Configure) screen fields (Continued)

Field	Description
Monitors	Monitor(s) being used to monitor the VPN connection Select one or more monitors. Notes: Factory-defined monitor — DefaultMonitor. This example should be replaced with your own monitor definition. To configure monitors, see WAN > Monitors > Configure on page 200.

E.4 WAN > WiFi Networks

The WiFi Networks tab is used to create and maintain configuration details for the Wi-Fi networks (access points) that the MG90 can connect to.

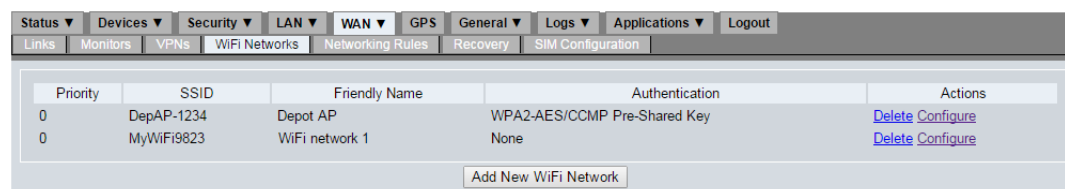


Figure E-18: LCI: WAN > WiFi Networks—Sample screen

Table E-17: WAN > WiFi Networks screen fields

Field	Description
Priority	Network Priority When more than one Wi-Fi network (access point) is defined, the network with the highest priority is connected first.
SSID	Basic Service Set Identifier The identifier broadcast by the access point.
Friendly Name	Descriptive name of the access point
Authentication	Authentication method used by the access point
Actions	Click these optional links to perform actions on the associated VPN profiles: - Delete — Delete the associated access point configuration. - Configure — Configure the details for the associated access point. See WAN > WiFi Networks > Add New WiFi Network/ Configure Network on page 211.

E.4.1 WAN > WiFi Networks > Add New WiFi Network/Configure Network

Status ▾ Devices ▾ Security ▾ LAN ▾ **WAN ▾** GPS ▾ General ▾ Logs ▾ Applications ▾ Logout
 Links Monitors VPNs WiFi Networks Networking Rules Recovery SIM Configuration

WiFi Network Configuration

General Settings:

Friendly Name:

SSID:

Probe Hidden SSID: ☒

Any BSSID: ☒

BSSID:

Default Network Priority: ☒

Priority:

Network Settings:

High Cost Link: ☐

Change Default MTU Size: ☐

MTU Size:

Auto Local IP: ☒

DHCP Assumes Same Network: ☐

Send hostname with DHCP: ☐ Disabled ☐ Send ESN ☐ Custom

Local IP Address:

Network Mask:

Gateway:

Masquerade: ☒

Masquerade Port Range: ☐ Automatic ☒ Manual

Automatic DNS: ☒

Primary DNS:

Secondary DNS Servers:

Use Management Tunnel: ☒

Pilot Ping: ☐

Monitors: ☒ DefaultMonitor

Monitor Mode:

VPN: ☒ VPN Configuration ☒ VPN Configuration_1 ☐ VPN Configuration_2

Connection Method: ☐ Connect One ☐ Random ☐ Round Robin - Alphanumeric Order ☒ Connect All

Split Access: ☐

Security Settings:

Protected Management Frames:

Encryption:

Authentication:

PEAP Version:

PEAP Label:

PEAP Inner Authentication:

WEP Key Size:

WEP Key:

Retype WEP Key:

WPA Pre-Shared Key:

Retype WPA Pre-Shared Key:

Identity:

Password:

Retype Password:

CA Certificate: No file chosen (installed)

Uninstall CA Certificate: ☐

Certificate Profile: ☐ J-Cert ☐ W-Cert ☐ default-Cert

Private Zone:

Enable Private Zone: ☒

Number of Private Zone:

Private Zone	Private Zone IP	Private Zone IP	Private Zone IP	Private Zone IP
Private Zone 1	testzone1.com	Private Zone IP 1	11.11.11.11	Delete
Private Zone 2	testzone2.com	Private Zone IP 2	22.22.22.22	Delete

Radio Frequency:

Band	Channels
☒ All	All
☐ 802.11a/n/ac	☐ All ☐ 36 : 5.18 GHz ☐ 40 : 5.2 GHz ☐ 44 : 5.22 GHz ☐ 48 : 5.24 GHz ☐ 149 : 5.745 GHz ☐ 153 : 5.765 GHz ☐ 157 : 5.785 GHz ☐ 161 : 5.805 GHz ☐ 165 : 5.825 GHz
☐ 802.11b/g/n	☐ All ☐ 1 : 2.412 GHz ☐ 2 : 2.417 GHz ☐ 3 : 2.422 GHz ☐ 4 : 2.427 GHz ☐ 5 : 2.432 GHz ☐ 6 : 2.437 GHz ☐ 7 : 2.442 GHz ☐ 8 : 2.447 GHz ☐ 9 : 2.452 GHz ☐ 10 : 2.457 GHz ☐ 11 : 2.462 GHz ☐ 12 : 2.467 GHz ☐ 13 : 2.472 GHz ☐ 14 : 2.484 GHz
☐ Public Safety	5MHz Only ☐ All ☐ 35 : 4.957 GHz ☐ 70 : 4.975 GHz ☐ 65 : 4.972 GHz ☐ 5 : 4.942 GHz ☐ 10 : 4.945 GHz ☐ 40 : 4.96 GHz ☐ 75 : 4.977 GHz ☐ 15 : 4.947 GHz ☐ 45 : 4.962 GHz ☐ 85 : 4.982 GHz ☐ 50 : 4.965 GHz ☐ 55 : 4.967 GHz ☐ 80 : 4.98 GHz ☐ 20 : 4.95 GHz ☐ 25 : 4.952 GHz ☐ 95 : 4.987 GHz ☐ 90 : 4.985 GHz ☐ 30 : 4.955 GHz ☐ 60 : 4.97 GHz

Figure E-19: LCI: WAN > WiFi Networks > Add New WiFi (or Configure) Network—Sample screen

Table E-18: WAN > WiFi Networks > Add New WiFi Network (or Configure) screen fields

Field	Description																			
General Settings																				
Friendly Name	Enter a descriptive nickname for the Wi-Fi network. This name identifies the network in other LCI screens (e.g. WAN > Links > Configure for a Wi-Fi radio that is provisioned to be used on WAN).																			
SSID	Wi-Fi network's Basic Service Set Identifier (Network display name) Enter the SSID of the Wi-Fi network to which the MG90 should connect.																			
Probe Hidden SSID	Connection requests allowed to access points not broadcasting SSIDs - Selected — If an access point is not broadcasting the SSIDs for its Wi-Fi networks, the MG90 can still request a connection using the SSID in the previous field (SSID). - Not selected — The MG90 cannot request a connection to an AP's Wi-Fi network if the SSID is not being broadcast.																			
Any BSSID	Connect to any access point broadcasting the SSID value (above). - Selected — MG90 will connect to any access point device with a broadcast SSID (BSSID) that matches the SSID field above. - Not selected — The MG90 will connect to an access point device that is broadcasting the SSID (from the field above) if the AP's MAC address is listed in the BSSID field below. This approach is more secure (will connect only to 'approved' APs).																			
BSSID	Enter the MAC address of the access point that the MG90 can connect to. <i>Note: This field is available only if Any BSSID is not selected.</i>																			
Default Network Priority	Network priority of this AP																			
Priority	When a Wi-Fi WAN link has more than one AP (with different SSIDs) selected, the AP network priorities are compared, and the link will connect to the AP with the highest priority. (Note — If multiple APs have the same (highest) priority, the MG90 uses the first one that is available.) - Selected — Use 0 (default value) for the network priority. - Not selected — Enter the network priority in the Priority field.																			
Security Settings																				
Protected Management Frames	Protected Management Frames for augmented WPA2 privacy Set the PMF option to work with the option used by the external Access Point to which the MG90's Wi-Fi network connects: <table><tr><th rowspan="2">MG90 PMF</th><th colspan="3">External access point PMF</th></tr><tr><th>Disabled</th><th>Optional</th><th>Required</th></tr><tr><td>Disabled</td><td>Connection allowed, PMF not used</td><td>Connection allowed, PMF not used</td><td>Connection not allowed</td></tr><tr><td>Optional</td><td>Connection allowed, PMF not used</td><td>Connection allowed, PMF may or may not be used</td><td>Connection allowed, PMF used</td></tr><tr><td>Required</td><td>Connection not allowed</td><td>Connection allowed, PMF used</td><td>Connection allowed, PMF used</td></tr></table> <i>Note: When enabled (Optional / Required), the Encryption is automatically set to WPA2-AES/CCMP.</i>	MG90 PMF	External access point PMF			Disabled	Optional	Required	Disabled	Connection allowed, PMF not used	Connection allowed, PMF not used	Connection not allowed	Optional	Connection allowed, PMF not used	Connection allowed, PMF may or may not be used	Connection allowed, PMF used	Required	Connection not allowed	Connection allowed, PMF used	Connection allowed, PMF used
MG90 PMF	External access point PMF																			
	Disabled	Optional	Required																	
Disabled	Connection allowed, PMF not used	Connection allowed, PMF not used	Connection not allowed																	
Optional	Connection allowed, PMF not used	Connection allowed, PMF may or may not be used	Connection allowed, PMF used																	
Required	Connection not allowed	Connection allowed, PMF used	Connection allowed, PMF used																	

Table E-18: WAN > WiFi Networks > Add New WiFi Network (or Configure) screen fields (Continued)

Field	Description
Encryption	Encryption method MG90 must use to connect to this network - None — No encryption, all Security Settings fields are disabled. - WEP - WPA-RC4/TKIP - WPA-AES/CCMP - WPA2-RC4/TKIP - WPA2-AES/CCMP (Default) <i>Note: If Protected Management Frames is enabled, Encryption is automatically set to WPA2-AES/CCMP.</i>
Authentication	Authentication protocol for the selected Encryption method - Open — Note that this option is not available if Protected Management Frames are enabled. - WPA-PSK - EAP-TLS — Note that you must ensure you select a valid CA Certificate when using this protocol. - EAP-PEAP <i>Note: Protocol availability depends on the selected encryption method. See Table E-19 on page 219 for details.</i> <i>Note: Security options required depend on the protocol. See Table E-20 on page 220 for details.</i>
PEAP Version	Version of PEAP (Protected Extensible Authentication Protocol) to use. Version 0 (Note — No other versions are supported.) <i>Note: This field is available only when Authentication method is EAP-PEAP.</i>
PEAP Label	Client encryption type to use. - Client EAP Encryption (old) - Client PEAP Encryption (new) <i>Note: This field is available only when Authentication method is EAP-PEAP.</i>
PEAP Inner Authentication	PEAP inner authentication algorithm to use. - MSCHAPv2 - GTC <i>Note: This field is available only when Authentication method is EAP-PEAP.</i>
WEP Key Size	Size of key to use. 40 bits 104 bits <i>Note: This field is available only when Encryption Method is WEP and Authentication protocol is Open.</i>
Change WEP Key	Select to access the next three fields <i>Note: This field appears only when Encryption method is WEP, and a WEP key is already in use.</i>
Previous WEP Key	Enter the current WEP Key being used. (Note that the value is obfuscated for security reasons.) <i>Note: This field is available only when Change WEP Key is selected.</i>

Table E-18: WAN > WiFi Networks > Add New WiFi Network (or Configure) screen fields (Continued)

Field	Description
WEP Key or New WEP Key	Enter the WEP Key (5 or 13 pairs of hexadecimal digits, no spaces), and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.).
Retype WEP Key or Retype New WEP Key	▪ If WEP Key Size = 40, enter 5 pairs of hexadecimal digits ▪ If WEP Key Size = 104, enter 13 pairs of hexadecimal digits <i>Note: These fields are available only when Encryption method is WEP.</i>
Change WPA Pre-Shared Key	Select to access the next three fields. <i>Note: This field appears only when using a form of WPA encryption, the Authentication method is WPA-PSK, and a WPA Pre-Shared Key is already in use.</i>
Previous WPA Pre-Shared Key	Enter the current WPA Pre-Shared Key. (Note that the value is obfuscated for security reasons.) <i>Note: This field is available only when Change WPA Pre-Shared key is selected.</i>
WPA Pre-Shared Key or New WPA Pre-Shared Key	Enter the WPA Pre-Shared Key provided by the Wi-Fi network's administrator, and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.).
Retype WPA Pre-Shared Key or Retype New WPA Pre-Shared Key	Valid formats: ▪ 8–63 printable ASCII characters ▪ 64 hexadecimal digits <i>Note: These fields are available only when Authentication method is WPA-PSK.</i>
Identity	Identity (for EAP protocol) needed to log on to this Wi-Fi network ▪ Format: ASCII string ▪ Required field <i>Note: These field is meaningful only when Authentication method is EAP-PEAP. Do not enter a value if Authentication method is EAP-TLS.</i>
Change Password	Select to access the next three fields. <i>Note: This field appears only when Authentication method is EAP-PEAP or EAP-TLS, and a Password is already in use.</i>
Previous Password	Enter the current Password. (Note that the value is obfuscated for security reasons.) <i>Note: This field is available only when Change Password is selected.</i>
Password or New Password	Enter the Password that the user Identity needs to log on to this Wi-Fi network, and re-enter it in the 'Retype' field to verify. (Note that the values are obfuscated for security reasons.).
Retype Password or Retype New Password	▪ Format: ASCII string <i>Note: These fields are available only when Authentication method is EAP-PEAP.</i>

Table E-18: WAN > WiFi Networks > Add New WiFi Network (or Configure) screen fields (Continued)

Field	Description
CA Certificate	Click Choose File to locate and open a CA certificate file (.pem) for the network, if supplied by the Wi-Fi network administrator. Important: Only one certificate file can be uploaded—the file must contain both the root and intermediate certificates. If the CSA (Certificate Signing Authority) provided separate root and intermediate certificates, combine them as described in Creating a combined CA certificate on page 92 before using Browse/Choose File. Note: You can upload the file from a device connected to the LAN. Note: This field is available only when Authentication method is EAP-PEAP or EAP-TLS.
Certificate Profile	Select a profile (which identifies a signed certificate) to use for authentication. The displayed profiles are defined in Certificate Management (Security > Certificate Management). For details, see Certificate Configuration on page 85.) Important: Do not select the desired profile if it is not yet completed—for example, if the MG90 is deployed before certificates are loaded. When the certificate profile is ready (CSR generated and certificate loaded), the AMM can be used to mass-configure VPNs and/or Wi-Fi networks on multiple MG90 routers with the new certificate. Note: This field is available only when Authentication method is EAP-PEAP or EAP-TLS.
Network Settings	
High Cost Link	High Cost Link - Selected—High cost link. Transmission of management data (e.g. log files uploads, automatic software downloads, etc.) is limited, with most of the data being held until a low cost link is active. (Note: If required, you can allow Auto software updates and firmware updates over high cost links, by setting appropriate options. See Table G-8, General > Auto Software Updates screen fields, on page 248 for details.) - Not selected—Not a high cost link. Note: Public Wi-Fi links are often declared as High Cost if the mobile network operator charges per MB.
Change Default MTU Size	Use a different MTU Size than the default (1500 bytes). - Selected—MTU Size field can be edited. (Default) Deselect this checkbox to reset the MTU Size to the default value (the value resets when you click Save). - Not selected—MTU Size field cannot be edited. Note: This may be required to accommodate some network configurations. Only change if advised by Sierra Wireless.
MTU Size	Maximum Transmission Unit size (in bytes) - Valid range: 256–1500 - Default: 1500
Auto Local IP	Enable DHCP for this interface. - Selected—Enabled. The IP address will be assigned by a DHCP server connected to the access point network. - Not selected—Not enabled. Assign the Local IP Address, Network Mask, and Gateway manually.

Table E-18: WAN > WiFi Networks > Add New WiFi Network (or Configure) screen fields (Continued)

Field	Description
DHCP Assumes Same Network	DHCP assignment when lease expires - Selected — Attempt to reconnect to same DHCP assignment when DHCP lease expires. - Not selected — Router will request an IP address from a DHCP server in the available network when the lease expires <i>Note: This field is available only when Auto Local IP is selected.</i>
Send Hostname with DHCP	Enable/disable sending of MG90-identifying information with DHCP request - Disabled — Do not send identifying information - Send ESN — Send the MG90's ESN (Electronic Serial Number) - Custom — Send a custom hostname (for example, "Bus401") to identify the MG90 to the DHCP server. <i>Note: This field is available only if Auto Local IP is selected.</i>
Local IP Address	Statically-assigned Local IP Address IPv4 address format (e.g. xxx.xxx.xxx.xxx) <i>Note: This field is available only when Auto Local IP is not selected.</i>
Network Mask	Network mask of the Local IP Address IPv4 netmask format (e.g. xxx.xxx.xxx.xxx) <i>Note: This field is available only when Auto Local IP is not selected.</i>
Gateway	Default gateway to use for the Local IP Address IPv4 address format (e.g. xxx.xxx.xxx.xxx) <i>Note: This field is available only when Auto Local IP is not selected.</i>
Masquerade	Network Address Translation for LAN-originated traffic leaving the MG90 WAN interface - Selected — Enabled. This is the typical setting. - Not selected — Disabled
Masquerade Port Range	Port range to use for masquerade (NAT) - Automatic — Enabled - Manual — Disabled (Default). This should be used in most cases to avoid using defined or reserved ports. <i>Note: This field is available only when Masquerade is selected.</i>
Minimum Port Number	Range of ports to use for masquerade (NAT) - Default range: 49152–65535 - Valid range: 0–65535 - If Minimum Port Number < 49152: - traffic on ports lower than 512 is mapped to other ports lower than 512 - traffic on ports 512 to 1024 is mapped to ports lower than 1024 - traffic on ports greater than 1024 is mapped to ports greater than 1024 <i>Note: These fields are available only when Masquerade is selected and Masquerade Port Range is Manual.</i>
Maximum Port Number	

Table E-18: WAN > WiFi Networks > Add New WiFi Network (or Configure) screen fields (Continued)

Field	Description
Automatic DNS	DNS servers to be used - Selected — Use DNS servers specified by DHCP server. - Not selected — Use the DNS servers specified in Primary DNS or Secondary DNS. The fastest-responding server (regardless of whether named as Primary or Secondary) is chosen as the server to use. Periodically, the servers are re-evaluated to make sure the fastest-responding server is being used. If private DNS servers are used, set up DNS zones — see Configuring DNS Zones for Private DNS Server Use on page 82 for details. <i>Note: This must be disabled (not selected) if using a static IP address.</i>
Primary DNS	IP address of primary domain name server - Format: IPv4 address (xxx.xxx.xxx.xxx) - Required field (when Automatic DNS is not selected) <i>Note: This field is available only when Automatic DNS is not selected.</i>
Secondary DNS Servers	IP addresses of secondary domain name servers - Format: IPv4 addresses, comma (e.g. xxx.xxx.xxx.xxx, yyy.yyy.yyy.yyy) - Optional field <i>Note: This field is available only when Automatic DNS is not selected.</i>
Use Management Tunnel	Management Tunnel usage The management tunnel is a dedicated secure VPN connection between the MG90 and AMM. - Selected — AMM can access the MG90. (Default) - Not selected — Do not use the management tunnel. AMM cannot access the MG90. To configure the management tunnel, see WAN > VPNs > (Management Tunnel) > Configure on page 202.
Pilot Ping	Pilot ping - Selected — Enabled. Before a WAN link is identified as established, the MG90 attempts to pass ping traffic over the link. If the ping succeeds, the link is identified as established. If the ping fails, the link is not established. - Not selected — Disabled (Default). Ping traffic is not attempted, which could result in a WAN link being identified as established although it may not be able to pass traffic. <i>Note: After a WAN link has been established, ping monitors (next field) are used to monitor the link's connection.</i>
Monitors	Monitor(s) being used to monitor the link's connection Select one or more monitors. Notes: Factory-defined monitor — DefaultMonitor. This example should be replaced with your own monitor definition; it is commonly blocked within enterprise networks. Use an enterprise-specific network. To configure monitors, see WAN > Monitors > Configure on page 200.

Table E-18: WAN > WiFi Networks > Add New WiFi Network (or Configure) screen fields (Continued)

Field	Description
Monitor Mode	Effect of selected monitors' state on link status - Success in one monitor keeps the link up — If at least one monitor is reporting as active, then the link should be considered 'up'. - Failure in one monitor declares the link down — If any one monitor is reporting as inactive, then the link should be considered 'down'. <i>Note: This field is meaningful only when one or more monitors are selected.</i>
VPN	VPNs that the WAN link can establish when the link is active - If multiple VPNs are selected, each of the VPNs must be LAN to LAN. - To configure VPNs, see WAN > VPNs on page 201. Warning: In the VPN field, if a VPN profile is selected that is configured as a full tunnel (subnet 0.0.0.0/0), do not select any other profiles. If the full tunnel profile and another profile are selected, none of the changes made to the screen will be saved when Save is clicked.
Connection Method	Number of VPN tunnels to establish for a WAN connection - Connect One — Only 1 tunnel established for the WAN link, using selected method below: - Random — Establish tunnel on a randomly selected VPN from the VPN list. If tunnel cannot be established or fails, use next randomly selected VPN. This results in basic (unmanaged) load balancing across VPN servers. - Round Robin - Alphanumeric Order — Establish tunnel on the first VPN (sorted by name) in the VPN list. If tunnel cannot be established or fails, use next VPN (in sorted order). This is a redundant failover method that does not have any load-balancing characteristics. - Connect All — Tunnels to all VPNs in the VPN list established simultaneously for the WAN link. <i>Note: This option (Connect All) can only be selected for LAN-to-LAN VPNs.</i> <i>Note: Any changes to Connection Method take effect after the next reboot.</i>
Split Access	Allow incoming session initiation on non-active connected link This allows an incoming session to initiate on a link even when the link is not the active (i.e. default route) link but is connected to the network. - Selected — Allowed - Not selected — Not allowed This is useful for applications such as live video look-in to a Wi-Fi interface even if the active connection is via another WAN (e.g. cellular). <i>Note: Users are encouraged to evaluate use of the Split Access feature from a security and system perspective prior to enabling. Depending on available links and routing rules, traffic may route from WAN to LAN or between WAN networks.</i>
Private Zone	
Enable Private Zone	Enables/disable DNS private zone use on this link. - Selected — Enabled. DNS private zones can be used on this link. - Not selected — Disabled. DNS private zones cannot be used on this link.
Number of Private Zone	Table of 1–10 private zone configuration entries
Private Zone <#>	Domain name to be resolved by the internal DNS server managing the private zone.

Table E-18: WAN > WiFi Networks > Add New WiFi Network (or Configure) screen fields (Continued)

Field	Description
Private Zone IP <#>	IP address of the internal DNS server managing the private zone.
Radio Frequency	
Band	Supported Wi-Fi bands Select the radio band this Wi-Fi network operates on — the MG90 will search these bands for the SSID to connect. Choose one of the following: - All — MG90 searches all bands for the SSID. (Default) 802.11a/n/ac 802.11b/g/n - Public Safety
Channels	Supported Channels for selected Bands Select the channels (frequencies) used by the Wi-Fi network on the selected Band — select 'All' or any combination of the listed channels. - All — All listed channels are supported. (Default) - Other channels — Select any combination of channels. (Note — You must deselect All before you can select any of the other channels.)

The following table summarizes the authentication methods available for each encryption option:

Table E-19: Summary of available authentication options

Encryption	Open	WPA-PSK	EAP-TLS	EAP-PEAP
none	-	-	-	-
WEP	X	-	X	X
WPA-RC4/TKIP	-	X	X	X
WPA-AES/CCMP	-	X	X	X
WPA-RC4/TKIP	-	X	X	X
WPA2-AES/COMP	-	X	X	X

The following table summarizes the applicable security fields for each authentication method:

Table E-20: Summary of required security options for each authentication method

Authentication	PEAP			WEP		WPA			Certificate		Private Key	
	Version	Label	Inner Authentication	Key Size	Key	Pre-Shared Key	Identity	Password	CA	Client	Key	Password
Open	-	-	-	-	-	-	-	-	-	-	-	-
WPA-PSK	-	-	-	-	-	X	-	-	-	-	-	-
EAP-TLS	-	-	-	-	-	-	X	-	X	X	X	X
EAP-PEAP	X	X	X	-	-	-	X	X	X	-	-	-

E.5 WAN > Networking Rules

The WAN Networking Rules tab is used to defined 'global' networking rules that apply to all WAN connections. The WAN rules include:

- Access Blocking
- Access Granting
- Port Forwarding
- QoS Prioritizing
- Routing Rules (Policy based)

Note: There are three 'levels' of networking rules — LAN segment, Global (WAN), and Global (LAN). If there is a conflict between any of these rules, LAN segment rules override Global WAN link and Global LAN rules, and Global WAN rules override Global LAN rules.

The WAN Networking Rules and LAN Networking Rules use similar setup parameters. For LAN networking rules, see [LAN > Networking Rules](#), and [LAN > LAN Segments > Networking Rules](#) on page 158.

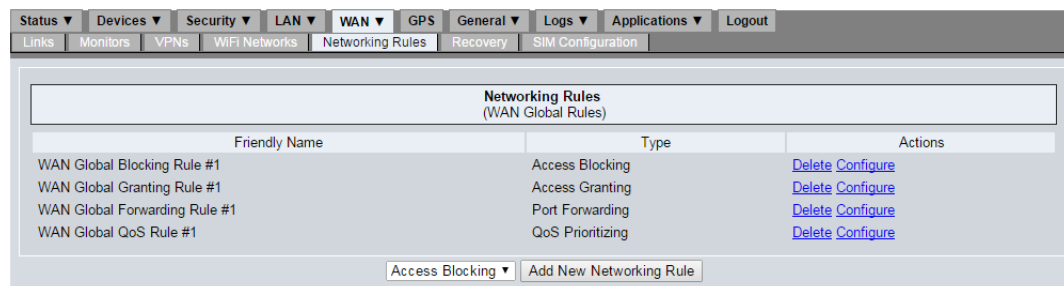


Figure E-20: LCI: WAN > Networking Rules—Sample screen

Table E-21: WAN > Networking Rules screen fields

Field	Description
Friendly Name	Descriptive name for the networking rule

Table E-21: WAN > Networking Rules screen fields (Continued)

Field	Description
Type	Rule type: - Access Blocking — Block incoming or outgoing traffic. See Access Blocking Rules on page 221. - Access Granting — Permit incoming or outgoing traffic. See Access Granting Rules on page 222. - Port Forwarding — Permit port forwarding. See Port Forwarding Rules on page 224. - QoS Prioritizing — Assign traffic priority. See QoS Priority Rules on page 224. - Routing Rule — Routes traffic to different WAN interfaces based on traffic characteristics. See Policy-Based Routing Rules on page 226.
Actions	Click these optional links to perform actions on the associated rules: - Delete — Delete the associated networking rule. - Configure — Configure the associated network rule.
Add New Networking Rule	From the drop-down, select the type of rule to add, and click Add New Networking Rule. For usage details, see Setting up the WAN Firewall on page 62.

Access Blocking Rules

Add an Access Blocking rule to block incoming or outgoing traffic (from the MG90's perspective) for a specific IP address, based on the criteria in [Table E-22](#) on page 221.

Tip: Fields that are left blank are treated as “wildcards.” Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.

The screenshot displays the 'Access Blocking Firewall Rule (WAN Global Rules)' configuration page. The form includes the following fields and values:

- Rule Name:** WAN Global Blocking Rule #1
- Direction:** Incoming (selected)
- Source IP Address:** 192.168.66.10
- Source Port Range:** 104 to 423
- Protocol:** TCP
- Destination IP Address:** 192.168.77.92
- Destination Port Range:** 1000 to 1319
- Action:** Reject (selected)
- Reject Cause:** Prohibited (selected)

Buttons for 'Save' and 'Cancel' are located at the bottom of the form.

Figure E-21: LCI: WAN > Networking Rules > Add Rule (Access Blocking)—Sample screen

Table E-22: WAN > Networking Rules > Add Rule (Access Blocking) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.

Table E-22: WAN > Networking Rules > Add Rule (Access Blocking) screen fields (Continued)

Field	Description
Direction	Traffic direction relative to the MG90 - Incoming — The Source IP Address will be blocked. - Outgoing — The Destination IP Address will be blocked.
Source IP Address	Source IP address - Format: [!]xxx.xxx.xxx.xxx[/xx] - Note: The optional '!' means "anything other than this address (or range)". - Examples: - Address without netmask—192.168.4.17. Applies to the stated IP address. - Address with netmask—192.168.4.0/24. Applies to the IP address range 192.168.4.0–192.168.4.255.
Source Port Range	Starting and ending source port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port
Protocol	Communications protocol - TCP - UDP - TCP/UDP - ICMP (Internet Control Message Protocol)
Destination IP Address	Destination IP address Format: xxx.xxx.xxx.xxx[/xx]
Destination Port Range	Starting and ending source port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port
Action	Action to take when traffic matches the rule's specifications: - Reject — Send the Reject Cause to the sender. - Drop — Drop the traffic packets without notice. <i>Note: The 'Drop' rule is useful when attempting to prevent hacking.</i>
Reject Cause	Reason that user receives when Action is set to 'Reject' - Prohibited — Inform user that site is banned. - Unreachable — Inform user that site is unreachable.

Access Granting Rules

Add an Access Granting rule to permit incoming or outgoing traffic (from the MG90's perspective) for a specific IP address, based on the criteria in [Table E-23](#) on page 223.

Tip: Fields that are left blank are treated as "wildcards." Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.

Note: By default, all ports (except ports 22 and 2222 (SSH)) to the MG90 from the WAN side are blocked. Access granting rules will not open additional ports to the MG90 but are designed to act as exceptions to access blocking rules.

Access Granting Firewall Rule
(WAN Global Rules)

Rule Name: WAN Global Granting Rule #1

Direction: ☐ Incoming ☒ Outgoing

Source IP Address: 192.168.88.240/32

Source Port Range: 200 204

Protocol: TCP

Destination IP Address: 192.168.109.24/32

Destination Port Range: 1730 1734

Save Cancel

Figure E-22: LCI: WAN > Networking Rules > Add Rule (Access Granting)—Sample screen

Table E-23: WAN > Networking Rules > Add Rule (Access Granting) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.
Direction	Traffic direction relative to the MG90 - Incoming — The Source IP Address will be granted. - Outgoing — The Destination IP Address will be granted.
Source IP Address	Source IP address - Format: [!]<i>xxx.xxx.xxx.xxx</i>[/<i>xx</i>] Note: The optional '!' means "anything other than this address (or range)". - Examples: - Address without netmask—192.168.4.17. Applies to the stated IP address. - Address with netmask—192.168.4.0/24. Applies to the IP address range 192.168.4.0–192.168.4.255
Source Port Range	Starting and ending source port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port
Protocol	Communications protocol - TCP - UDP - TCP/UDP - ICMP (Internet Control Message Protocol)
Destination IP Address	Destination IP address Format: [!]<i>xxx.xxx.xxx.xxx</i>[/<i>xx</i>] Note: The optional '!' means "anything other than this address (or range)".
Destination Port Range	Starting and ending source port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port

Port Forwarding Rules

Add a Port Forwarding rule to permit traffic from the WAN interface (Source IP + Destination Port Range) to be forwarded to a specific IP address and port on the LAN interface (Forward to Host and Forward Port Range).

Tip: Fields that are left blank are treated as “wildcards”. Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.

The screenshot shows the 'Port Forwarding Firewall Rule' configuration window. The title bar indicates it's for 'WAN Global Rules'. The form contains the following fields and values:

- Rule Name:** WAN Global Forwarding Rule #1
- Source IP:** 192.168.101.0
- Destination Port Range:** 400 to 415
- Protocol:** TCP
- Forward to Host:** 192.168.66.10
- Forward Port Range:** 140 to 155

Buttons for 'Save' and 'Cancel' are located at the bottom right of the form.

Figure E-23: LCI: WAN > Networking Rules > Add Rule (Port Forwarding)—Sample screen

Table E-24: WAN > Networking Rules > Add Rule (Port Forwarding) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.
Source IP	IP address of sender - Format: xxx.xxx.xxx.xxx[/xx] - If forwarding only based on the destination port(s), leave this field blank.
Destination Port Range	Starting and ending destination port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port
Protocol	Communications protocol - TCP - UDP - TCP/UDP
Forward to Host	Local IP Address of host. - Static IP address - Format: xxx.xxx.xxx.xxx
Forward Port Range	Starting and ending port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port

QoS Priority Rules

Add QoS priority rules to various applications used by the customer and guarantee a certain level of performance to data flow.

Tip: Fields that are left blank are treated as “wildcards”. Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.

For applications that do not have a predetermined destination IP address such as Voice-over-IP, using the Source IP Address and Source Port is supported.

The screenshot shows the 'QoS Priority Rule (WAN Global Rules)' configuration window. It includes a navigation bar at the top with tabs like Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below this is a sub-menu bar with Links, Monitors, VPNs, WiFi Networks, Networking Rules, Recovery, and SIM Configuration. The main configuration area contains the following fields:

- Rule Name:** WAN Global Rule Name #1
- Destination Address/Netmask:** 208.81.125.0/24 (CIDR notation a.b.c.d[/x])
- Destination Port Range:** Start 2048 End(Optional) 4096
- Protocol:** TCP/UDP
- Source Address/Netmask:** 10.1.60.0/24 (CIDR notation a.b.c.d[/x])
- Source Port Range:** Start 2048 End(Optional) 4096
- Priority:** 0 (Smaller numbers have greater priority)
- DSCP Value:** EF (Default is CS0 (IP precedence 0))
- Minimum Guaranteed Bandwidth:** No guarantee
- Maximum Allowed Bandwidth:** Use available

At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure E-24: LCI: WAN > Networking Rules > Add Rule (QoS Prioritizing)—Sample screen

Table E-25: WAN > Networking Rules > Add Rule (QoS Prioritizing) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.
Destination Address/Netmask	Application server IP address - Format: [!]<i>xxx.xxx.xxx.xxx</i>[/<i>xx</i>] (CIDR notation) - Note: The optional '!' means “anything other than this address (or range)”. - Leaving this field blank gives priority to all traffic on this port, based on existing firewall rules.
Destination Port Range	Destination port number (For TCP, UDP, TCP/UDP Protocols) - Single port used for data transport (Start), or range of ports (Start/End) - End port is Optional - Valid values: 0–65535 <i>Note: This field is available only if Protocol type is TCP, UDP, or TCP/UDP.</i>
Protocol	Data transport protocol - ALL - TCP/UDP - TCP - UDP - ICMP
Source Address/Netmask	Source IP address (used for applications that do not have a predetermined IP address (e.g. VoIP)) - Format: [!]<i>xxx.xxx.xxx.xxx</i>[/<i>xx</i>] (CIDR notation) - Note: The optional '!' means “anything other than this address (or range)”.

Table E-25: WAN > Networking Rules > Add Rule (QoS Prioritizing) screen fields (Continued)

Field	Description
Source Port Range	Source port number (used for applications that do not have a predetermined IP address (e.g. VoIP)) - Single port used for data transport (Start), or range of ports (Start/End) - End port is Optional - Valid values: 0–65535 <i>Note: This field is available only if Protocol type is TCP, UDP, or TCP/UDP.</i>
Priority	Traffic priority Traffic to the WAN in the specified port and destination IP address is prioritized using this value. - Format: Integer - Minimum value: 0 (Highest priority) - Higher values are lower priority
DSCP Value	DSCP (Differentiated Services Code Point), also known as PNTM (Private Network Traffic Management) for Verizon - Select appropriate DSCP value from list. For DSCP details, refer to RFC 2597 and RFC 3260. - Values in the list are sorted from lowest priority (CS0) to highest priority (EF). - Value is used to prioritize traffic for end-to-end QoS across all devices in the path (if DSCP is supported).
Minimum Guaranteed Bandwidth	Minimum data transfer rate - No guarantee — No minimum data transfer rate. (Default) - Rate — Specify the minimum data rate (including the transfer unit) that should be provided <i>Note: If minimum bandwidth is specified for some rules, consider adding it to all rules. When the sum of the minimum guaranteed bandwidths for all transmissions is greater than the available bandwidth, transmissions with no guarantee will be stalled.</i>
Maximum Allowed Bandwidth	Maximum data transfer rate - Use available — No maximum data rate. (Default) - Rate — Specify the maximum data rate (including the transfer unit) that can be used. The maximum allowed bandwidth is used to ensure that traffic matching the condition specified by the rule does not exceed this bandwidth.

Policy-Based Routing Rules

Add a policy-based Routing Rule to allow routing of specific traffic to different WAN interfaces instead of the active WAN interface, based on the criteria in [Table E-26](#) on page 227.

Important:

- If two or more rules 'overlap', the rule with the higher priority (lowest Priority score) takes precedence.
- The system supports the use of either policy based routing rules or advanced routing rules, but not both. If setting up policy based rules, make sure to remove any existing advanced routing rules ([General > Advanced Routing Rules](#) on page 245).
- If an existing policy based rule is modified, the updated rule is used for any new data sessions; the original rule continues to be used (until the next system boot) for any data sessions that were using it when it changed.

The screenshot shows the 'Routing Rule (WAN Global Rules)' configuration window. The fields are as follows:

- Rule Name:** HTTP Traffic Rule
- Protocol:** TCP/UDP
- Destination Address/Netmask:** (blank)
- Destination Port Range:** Start (blank), End (blank)
- Source Address/Netmask:** 172.22.0.0/16
- Source Port Range:** Start: 80, End: 80
- Interface:** Sierra Wireless MC74XX @ MiniCard USB3 CB (Cellular B)
- Priority:** 0
- Failover:** (checkbox, unchecked)

Buttons at the bottom: Save, Cancel.

Figure E-25: LCI: WAN > Networking Rules > Add Rule (Routing Rule)—Sample screen

Tip: Fields that are left blank are treated as “wildcards”. Limit the use of wildcards (fill fields with appropriate values) to make sure your rule works as intended.

Table E-26: WAN > Networking Rules > Add Rule (Routing Rule) screen fields

Field	Description
Rule Name	Descriptive name for the networking rule.
Protocol	Communications protocol - ALL - TCP - UDP - TCP/UDP - ICMP (Internet Control Message Protocol)
Destination Address/Netmask	Destination IP address - Format: [!]<i>xxx.xxx.xxx.xxx</i>[/<i>xx</i>] - Note: The optional ‘!’ means “anything other than this address (or range)”. - Examples: - Address without netmask—192.168.4.17. Applies to the stated IP address. - Address with netmask—192.168.4.0/24. Applies to the IP address range 192.168.4.0–192.168.4.255.
Destination Port Range	Starting and ending source port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port <i>Note: This field is available only if Protocol type is TCP, UDP, or TCP/UDP.</i>

Table E-26: WAN > Networking Rules > Add Rule (Routing Rule) screen fields (Continued)

Field	Description
Source Address/ Netmask	Source IP address - Format: [!]xxx.xxx.xxx.xxx[/xx] - Note: The optional '!' means "anything other than this address (or range)". - Examples: - Address without netmask—192.168.4.17. Applies to the stated IP address. - Address with netmask—192.168.4.0/24. Applies to the IP address range 192.168.4.0–192.168.4.255. <i>Note: Rules using different protocols can use the same (or overlapping) source addresses. Make sure to use the Priority to indicate the preferred order (precedence) for overlapping rules.</i>
Source Port Range	Starting and ending source port numbers - Valid values: 0–65535 - Start port must be less than or equal to the end port <i>Note: This field is available only if Protocol type is TCP, UDP, or TCP/UDP.</i>
Interface	WAN link to which this rule applies The dropdown list shows all enabled WAN links.
Priority	Traffic priority Traffic to the WAN in the specified port and destination IP address is prioritized using this value. - Format: Integer - Minimum value: 0 (Highest priority) - Higher values are lower priority
Failover	Reroute traffic to next available interface if target interface link is down. - Selected — Traffic reroutes. - Not selected — Traffic is dropped.

E.6 WAN > Recovery

The Recovery tab is used to configure the MG90 to reboot after a WAN link has been down for a specified time period, and to restore the MG90's configuration if an update pushed from AMM caused the WAN link to go down.

The screenshot shows the 'WAN > Recovery' configuration screen. At the top, there is a navigation bar with tabs: Status, Devices, Security, LAN, WAN (selected), GPS, General, Logs, Applications, and Logout. Below the navigation bar, there is a sub-navigation bar with tabs: Links, Monitors, VPNs, WiFi Networks, Networking Rules, Recovery (selected), and SIM Configuration. The main content area is titled 'WAN Link Recovery' and contains two sections. The first section, 'WAN Link Recovery', has a checked checkbox and an input field with the value '600'. The second section, 'Remote Configuration WAN Recovery', also has a checked checkbox and an input field with the value '120'. At the bottom of the screen, there are 'Save' and 'Cancel' buttons.

Figure E-26: LCI: WAN > Recovery—Sample screen

Table E-27: WAN > Recovery screen fields

Field	Description
WAN Link Recovery	Enable/disable automatic reboot to reestablish WAN link - Selected — Enabled. The MG90 will automatically reboot if there is no WAN communication (WAN links are down) for the period in Reboot System After. - Not selected — Disabled. MG90 will not automatically reboot.
Reboot System After (secs)	Interval to wait before automatic reboot Enter the amount of time (in seconds) that the MG90 waits after losing a WAN connection before automatically rebooting. <i>Note: This field is available only if WAN Link Recovery is selected.</i>
Remote Configuration WAN Recovery	Enable/disable configuration change reversion If enabled and AMM pushes configuration changes that cause the MG90 to lose WAN connectivity, the changed configuration reverts to its original (pre-push) configuration. - Selected — Enabled. The MG90 discards AMM-pushed changes. - Not selected — Disabled. The MG90 does not discard AMM-pushed changes.
Restore previous configuration after (secs)	Interval to wait before restoring previous configuration Enter the amount of time (in seconds) that the MG90 keeps new configuration parameters pushed by AMM that result in losing WAN connectivity. If the MG90 has no WAN connectivity after the timer expires, the MG90 will revert to the original configuration. <i>Note: This field is available only if Remote Configuration WAN Recovery is selected.</i>

E.7 WAN > SIM Configuration

The SIM Configuration tab is used to indicate which SIM slots are used for each installed cellular radio.

The screenshot shows the 'SIM Configuration' screen within the 'WAN' tab. The interface includes a top navigation bar with tabs like Status, Devices, Security, LAN, WAN, GPS, General, Logs, Applications, and Logout. Below this, there's a sub-navigation bar with links for Links, Monitors, VPNs, WiFi Networks, Networking Rules, Recovery, and SIM Configuration. The main content area is titled 'SIM Configuration' and contains two rows: 'Cellular A SIM Slot' with a dropdown menu showing 'A1', and 'Cellular B SIM Slot' with a dropdown menu showing 'B1'. At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

Figure E-27: LCI: WAN > SIM Configuration—Sample screen

Table E-28: WAN > SIM Configuration screen fields

Field	Description
Cellular A SIM Slot	Select the slot that contains the SIM for the Cellular A radio. - A1 - A2
Cellular B SIM Slot	Select the slot that contains the SIM for the Cellular B radio. - B1 - B2

F: GPS Tab

This chapter describes the GPS tab, which allows you to identify the GPS source the MG90 uses, and to configure GPS reporting options.

The screenshot displays the 'GPS Configuration' tab in the LCI interface. The top navigation bar includes tabs for Status, Devices, Security, LAN, WAN, GPS (selected), General, Logs, Applications, and Logout. The main configuration area is titled 'GPS Configuration' and includes an 'Expand All' link. The 'Enable' checkbox is checked. The 'GPS Sources' section shows 'Built-in GPS' selected, with 'Enable Jitter Filter' and 'Enable DR' checkboxes. The 'External GPS via UDP Port' section has 'Source Name' set to 'ExtUDP' and 'UDP Port' set to '5068'. The 'External GPS via Serial or USB' section has 'Source Name' set to 'ExtSerial' and 'Device Attachment' set to 'Rear Panel Serial'. The 'NMEA Messaging' section has 'Local' and 'Remote' tabs. The 'Local' tab shows 'Sentences' set to 'GSV, GGA, RMC' and 'Report Interval' set to '5'. The 'Remote' tab shows 'Report Interval' set to '10'. The 'Additional Options' section for NMEA has 'Emit ESN in Proprietary Sentence' and 'Group Sentences in a Single UDP Packet' checkboxes. The 'TAPI Messaging' section has 'Local' and 'Remote' tabs. The 'Local' tab shows 'Responses' set to '30' and 'Report Interval' set to '30'. The 'Additional Options' section for TAPI has 'Enable' checkbox, 'Top of Hour' set to '0', 'Checksum' checked, 'CR/LF' checked, and 'Vehicle ID' set to '~'. The 'Local Forwarding' section has 'TCP', 'UDP', and 'Serial' tabs. The 'TCP' tab shows 'Listen Port' set to '9345'. The 'UDP' tab shows 'Broadcast LAN' checked and 'Port' set to '5067'. The 'Serial' tab shows 'RS-232' checked, 'Speed' set to 'B9600', 'DataBits' set to 'CS8', 'Parity' set to 'none', 'StopBitX2' checked, and 'HW Flow' checked. The 'Remote Forwarding' section has a text area for 'Remote client entries separated by spaces with format: <ip or hostname>:<port> or <ip or hostname>:<port>#<report interval [1,3600]>'. The 'Forwarding Thresholds' section has 'Enable' checkbox. The 'Time' tab shows 'Slow Report Interval (secs)' set to '30' and 'Fast Report Interval (secs)' set to '5'. The 'Speed' tab shows 'Speed Unit' set to 'mph * km/h' and 'Speed Change Threshold' set to '10'. The 'Distance' tab shows 'Distance Unit' set to 'yard * meter' and 'Distance Change Threshold' set to '100'. The 'Event Thresholds' section has 'Time', 'Speed', and 'Distance' tabs. The 'Time' tab shows 'Fastest Report Interval(secs)' set to '5'. The 'Speed' tab shows 'Speed Unit' set to 'mph * km/h', 'Critical Speed Threshold' set to '16', and 'High Speed Threshold' set to '3'. The 'Distance' tab shows 'Distance Unit' set to 'yard * meter', 'Critical Distance Threshold' set to '100', and 'High Distance Threshold' set to '20'. The 'Accuracy Unit' section has 'Accuracy Unit' set to 'yard * meter', 'Critical Accuracy Threshold' set to '5', and 'Critical Accuracy Interval (secs)' set to '30'. The 'Critical SBAS Status Event Reporting' checkbox is checked, and 'Critical SBAS Interval (secs)' is set to '30'. The 'Turn Based Forwarding & Reporting' section has 'Enable' checkbox. The 'Time' tab shows 'Turn Report Interval (secs)' set to '1'. The 'Rotation Speed' tab shows 'Rotation Threshold (degrees/sec)' set to '4.0'. A 'Submit' button is at the bottom.

Figure F-1: LCI: GPS—Sample screen

Note: The MG90 supports both National Marine Electronics Association (<http://www.nmea.org/>) and Trimble ASCII Interface Protocol (TAIP) messages. When configuring GPS, make sure to choose the correct NMEA and/or TAIP sentences for the applications that they will be sent to.

Table F-1: GPS screen fields

Field	Description
Enable	Enable/disable custom GPS configuration - Selected — Enabled - Not selected — Disabled (Note — All fields on the screen are disabled.)
GPS Sources Select the appropriate GPS source — Built-in GPS, External GPS via UDP Port, or External GPS via Serial or USB. (Only one can be selected — Built-in GPS is the default.)	
Built-in GPS	Internal GPS - Selected — MG90 uses the internal GPS device. (Default) - Not selected — Not used
Enable Jitter Filter	Jitter filter - Selected — Enabled. Location changes when speed is < 1.5 km/h are dropped to overcome GNSS erroneous data when the MG90 is stationary. - Not selected — Disabled (Default). All location changes are reported. <i>Note: This field is available only if Built-in GPS is selected.</i>
Enable DR	GPS Dead Reckoning - Selected — Enabled. Calibration will begin automatically when vehicle begins moving. See Configuring Dead Reckoning on page 97 for details. - Not selected — Disabled <i>Note: This field is available only if Built-in GPS is selected.</i>
Clear Calibration Data (button)	Clear previous Dead Reckoning calibration settings and immediately begin recalibrating. <i>Note: This button is available only if Enable DR is selected.</i>
External GPS via UDP Port	External GPS connected to UDP port - Selected — MG90 uses the external GPS device. - Not selected — Not used
Source Name	Descriptive name of the GPS device (appears in Status > General). Default: ExtUDP <i>Note: This field is available only if External GPS via UDP Port is selected.</i>
UDP Port	UDP port used by external GPS Default: 5068 <i>Note: This field is available only if External GPS via UDP Port is selected.</i>
External GPS via Serial or USB	External GPS connected to Serial or USB port - Selected — MG90 uses the external GPS device. <i>Note: Ensure the Serial Port in Devices > Serial is set to GPS in the Use field.</i> - Not selected — Not used

Table F-1: GPS screen fields (Continued)

Field	Description
Source Name	Descriptive name of the GPS device (appears in Status > General). Default: ExtSerial <i>Note: This field is available only if External GPS via Serial or USB is selected.</i>
Device Attachment	Physical port used by GPS device - Rear Panel Serial — The MG90's DB9 serial port. - USB Port — Either of the MG90's USB ports on the rear panel. <i>Note: This field is available only if External GPS via Serial or USB is selected.</i>
NMEA Messaging	
<i>Note: Local and remote consumers (devices 'listening' for GPS messages) can both be defined.</i>	
Local	
Sentences	Supported NMEA sentences for Local messages Enter a comma-separated list of supported NMEA sentences. Available sentences (as defined in the NMEA 0183 specification) are: - GGA: Global Positioning System Fix Data - GLL: Geographical Position, Latitude/Longitude - GSA: GPS DOP and active satellites - GSV: GPS Satellites in view - RMC: Recommended minimum specific GPS/TRANSIT data - VTG: Track Made Good and Ground Speed - ZDA: UTC Date/Time and Local Time Zone Offset
Report Interval	Interval between local NMEA message submissions Enter the number of seconds to wait between sending each NMEA message. Default: 5
Remote	
Sentences	Supported NMEA sentences for Remote messages Enter a comma-separated list of supported NMEA sentences. Available sentences (as defined in the NMEA 0183 specification) are: - GGA: Global Positioning System Fix Data - GLL: Geographical Position, Latitude/Longitude - GSA: GPS DOP and active satellites - GSV: GPS Satellites in view - RMC: Recommended minimum specific GPS/TRANSIT data - VTG: Track Made Good and Ground Speed - ZDA: UTC Date/Time and Local Time Zone Offset
Report Interval	Interval between remote NMEA message submissions Enter the number of seconds to wait between sending each NMEA message. Default: 10

Table F-1: GPS screen fields (Continued)

Field	Description
Additional Options	
Emit ESN in Proprietary Sentence	Enable/disable sending a proprietary NMEA sentence with ESN - Selected — Enabled - Not selected — Disabled
Group Sentences in a Single UDP Packet	Enable/disable sending of all NMEA sentences in a single packet - Selected — Enabled - Not selected — Disabled
TAIP Messaging <i>Local and remote consumers (devices 'listening' for GPS messages) can both be defined.</i>	
Local	
Responses	Supported TAIP responses for Local messages Enter a comma-separated list of supported TAIP responses. Available responses are: - AL: Altitude/Up Velocity - CP: Compact Position Solution - ID: Identification Number - LN: Long Navigational Message - PV: Position/Velocity Solution - ST: Status - TM: Time/Date
Report Interval	Interval between local TAIP message submissions Enter the number of seconds to wait between sending each TAIP message. Default: 30
Remote	
Responses	Supported TAIP responses for Remote messages Enter a comma-separated list of supported TAIP responses. Available responses are: - AL: Altitude/Up Velocity - CP: Compact Position Solution - ID: Identification Number - LN: Long Navigational Message - PV: Position/Velocity Solution - ST: Status - TM: Time/Date
Report Interval	Interval between remote TAIP message submissions Enter the number of seconds to wait between sending each TAIP message. Default: 30
Additional Options	
Enable	Enable/disable additional TAIP Messaging options - Selected — Enabled - Not selected — Disabled
Top of Hour	N/A

Table F-1: GPS screen fields (Continued)

Field	Description
Checksum	Enable/disable inclusion of checksum in TAIP messages Enable this option if the application that is receiving the data requires checksums to ensure data integrity. - Selected — Enabled. Include checksums. - Not selected — Disabled. Do not include checksums. <i>Note: This field is available only if Enable is selected.</i>
CR/LF	Enable/disable inclusion of CR/LF (Carriage Return and Line Feed) in TAIP messages Enable this option if the application that is receiving the data requires each reply on a new line. - Selected — Enabled. Include CR/LF. - Not selected — Disabled. Do not include CR/LF. <i>Note: This field is available only if Enable is selected.</i>
Vehicle ID	Unique vehicle identification code If required, enter a unique identification code that will be included with each TAIP response. This is useful in cases where a single monitoring system is receiving traffic from multiple devices. Length — 4 alpha-numeric characters (Note: If the code is 1–3 characters, it is automatically padded with spaces.) <i>Note: This field is available only if Enable is selected.</i>
Local Forwarding Data can be sent via TCP, UDP, and Serial (RS-232).	
TCP Use of TCP clients is discouraged since a poorly behaved client can block connections and impede operation of the GPS system. The MG90 does not enforce a minimum value (fastest forwarding) but intervals faster than five seconds are not recommended.	
Listen Port	Local consumer TCP listen port - Default port: 9345 - Valid range: 0–65535
UDP	
Broadcast LAN	Enable/disable UDP broadcast - Selected — Enabled - Not selected — Disabled (Default)
Port	UDP port - Default port: 5067 - A valid port value must be entered.

Table F-1: GPS screen fields (Continued)

Field	Description
Serial To receive data via the serial port: - Assign the serial port to GPS in Devices > Serial. - Connect a null modem cable with a DB9 connector to the gateway and the terminal. - Change the communication parameters below to match the terminal communication specification.	
RS-232	Enable/disable serial data forwarding via RS-232 port - Selected — Enabled - Not selected — Disabled (Default)
Speed	Serial port speed Select the appropriate speed from the drop-down.
DataBits	Serial port data bits Select the appropriate number of bits from the drop-down.
Parity	Serial port parity Select the appropriate parity from the drop-down.
StopBitX2	Serial port stop bits - Selected — 2 stop bits - Not selected — 1 stop bit
HW Flow	Serial port hardware flow control - Selected — Enabled - Not selected — Disabled
Remote Forwarding (...)	
Server List	Remote consumer server list - Space-separated list of IP addresses, ports, and report intervals (optional) - Format: <ip or hostname>:<port> Example: 10.0.0.12:5777 10.0.0.15:5777 <ip or hostname>:<port>#<report_interval[1,3600]> Example: 10.0.0.12:5777 10.0.0.15:5777#30
Forwarding Thresholds Forwarding thresholds define the rules for enabling variable interval reporting for NMEA and TAIP messaging, based on speed, distance, and elapsed time.	
Time	
Slow Report Interval (secs)	Maximum interval between reports, regardless of speed and distance threshold limits.
Fast Report Interval (secs)	Minimum interval between reports, regardless of speed and distance threshold limits.
Speed	
Speed Unit	Unit of speed measurement (mph or km/h)

Table F-1: GPS screen fields (Continued)

Field	Description
Speed Change Threshold	Speed increase/decrease (since last report) at which point report should be forwarded (subject to Fast Report Interval).
Distance	
Distance Unit	Unit of distance measurement (yard or meter)
Distance Change Threshold	Change in position (since last report) at which point report should be forwarded (subject to Fast Report Interval).
Event Thresholds Event thresholds affect when and how frequently the MG90 reports GPS events to AMM. These thresholds are based on time, speed, and distance. High and Critical thresholds are defined for speed and distance. For low-cost WAN links, the MG90 sends GPS information when a High threshold is crossed; for high-cost WAN links, the MG90 sends GPS information when a Critical threshold is crossed.	
Time	
Fastest Report Interval (secs)	Minimum interval between GPS event reports Set the minimum interval (in seconds) between GPS report submissions. If a report is ready to be sent due to a speed or distance threshold being crossed, the report will not be sent until this minimum interval has been reached. <i>Note: The MG90 does not enforce a minimum value (fastest forwarding) but intervals faster than five seconds are not recommended.</i>
Speed	
Speed Unit	Unit of measurement for vehicle speed Select mph or km/h.
Critical Speed Threshold	High-cost WAN link critical speed threshold Speed at which a GPS event is reported for a high-cost WAN link.
High Speed Threshold	Low-cost WAN link high speed threshold Speed at which a GPS event is reported for a low-cost WAN link.
Distance	
Distance Unit	Unit of measurement for distance traveled Select yard or meter.
Critical Distance Threshold	High-cost WAN link critical distance threshold Distance traveled at which a GPS event is reported for a high-cost WAN link.
High Distance Threshold	Low-cost WAN link high distance threshold Distance traveled at which a GPS event is reported for a low-cost WAN link.
Accuracy Unit	Unit of measurement for the Critical Accuracy Threshold field (see below). Select yard or meter. Default: meter

Table F-1: GPS screen fields (Continued)

Field	Description
Critical Accuracy Threshold	Position change threshold If the GPS position changes by more than this distance within the Critical Accuracy Interval, a GPS event is reported. Default: 5
Critical Accuracy Interval (secs)	Critical accuracy interval Number of seconds over which critical accuracy threshold is considered. - Minimum: >0 - Default: 30
Critical SBAS Status Event Reporting	Report SBAS events to AMM When enabled, SBAS (Satellite Based Augmentation System) events are reported to AMM. - Selected — Enabled - Not selected — Not enabled
Critical SBAS Interval (secs)	Minimum interval between SBAS event reports Set the minimum interval (in seconds) between SBAS report submissions. - Minimum: 1 - Default: 30
Turn Based Forwarding & Reporting Turn based forwarding ensures the MG90 will report GPS events to AMM while a vehicle is turning, during which the vehicle may not meet Speed or Distance Event Thresholds.	
Enable	Enable/disable turn-based forwarding and reporting - Selected — Enabled - Not selected — Disabled (Note — All fields in the section are disabled.)
Turn Report Interval (secs)	Maximum interval between GPS event reports Set the maximum interval (in seconds) between GPS report submissions while the vehicle is turning. <i>Tip: Set the Turn Report Interval lower (higher resolution) to capture more accurate data, which will provide the application receiving the data with a more complete path of travel during the turn.</i> - Range: 1–3600 - Default: 1
Rotation Threshold (degrees/secs)	Rotational speed at which a report is generated. - Range: 0.0–360.0 - Default: 4.0

G: General Tab

This chapter describes the General tab.

The General tab includes the following sub-tabs:

- Startup — Configure the MG90's startup behavior when ignition is turned on. See [General > Startup](#) on page 238.
- Shutdown — Configure the MG90's shutdown (and restart) behavior. See [General > Shutdown](#) on page 239.
- Services — Configure Event Reporting. See [General > Services](#) on page 240.
- Tools — Run a variety of diagnostic and other tools. See [General > Tools](#) on page 242.
- Backup/Restore — Backup and restore the MG90's current configuration. See [General > Backup/Restore](#) on page 244.
- Advanced Routing Rules — Enter custom scripts to run at specific times. See [General > Advanced Routing Rules](#) on page 245.
- Auto Software Updates — Configure the MG90's behavior for downloading software updates. See [General > Auto Software Updates](#) on page 247.

G.1 General > Startup

The Startup tab is used to control the MG90's startup behavior when power is applied.

The screenshot shows the LCI configuration interface. At the top is a navigation bar with tabs: Status, Devices, Security, LAN, WAN, GPS, General (selected), Logs, Applications, and Logout. Below this is a sub-tab bar with: Startup (selected), Shutdown, Services, Tools, Backup/Restore, and Advanced Routing Rules. The main content area is titled 'Startup Configuration'. It contains two settings: 'AutoPower' with a checked checkbox, and 'Delay After Ignition On (secs)' with a text input field showing '5' and a range '(0 secs - 255 secs)'. At the bottom of the configuration area are 'Save' and 'Cancel' buttons.

Figure G-1: LCI: General > Startup—Sample screen

Table G-1: General > Startup screen fields

Field	Description
AutoPower	MG90 startup behavior when power is applied ▪ Selected — Start automatically. (Default) ▪ Not selected — Start when Reset button is pressed.
Delay After Ignition On (secs)	Wait time between ignition on and power applied Enter the number of seconds of wait time before turning on the MG90's power after the ignition is turned on. ▪ Range: 0–255 ▪ Default: 0

G.2 General > Shutdown

The Shutdown tab is used to configure the MG90's shutdown behavior.

Shutdown Configuration

High Voltage (volts) (0.0v - 50.0v)

Low Voltage (volts) (0.0v - 50.0v)

Low Voltage Alarm Hysteresis (0.5v - 1.5v)

High Temperature (°C)

Low Temperature (°C)

Uptime Extension After Ignition Off (hrs) (0 - 25.5)

Button Reset Time (secs) (0 sec - 255 sec)

Figure G-2: LCI: General > Shutdown—Sample screen

Table G-2: General > Shutdown screen fields

Field	Description
High Voltage (volts)	Upper voltage threshold Enter the upper voltage threshold (in volts). The MG90 will shut down if the voltage exceeds this threshold. - Range: 0.0–50.0 - Default: 36.0 <i>Note: Voltage readings are subject to cable length and will always be slightly lower than the voltage measured at the source.</i>
Low Voltage (volts)	Lower voltage threshold Enter the lower voltage threshold (in volts). The MG90 will shut down if the voltage drops below this threshold to prevent further discharge of the vehicle battery. - Range: 0.0–50.0 - Default: 11.0 <i>Note: This is the "slow discharge" shutdown. When a vehicle cranks, the ignition system should conform to SAE J537. If it does not and the voltage spikes down below the SAE minimum, the MG90 will reboot, regardless of this setting. Also, voltage readings are subject to cable length and will always be slightly lower than the voltage measured at the source.</i>
Low Voltage Alarm Hysteresis	Low voltage hysteresis required for restart Enter the hysteresis value (in volts). After the MG90 shuts down due to low voltage, it will not restart until the input voltage exceeds Low Voltage + Low Voltage Alarm Hysteresis. This ensures the MG90 does not continually shutdown and restart when voltage is fluctuating around the low voltage value. - Range: 0.5–1.5 - Default: 0.9
High Temperature (°C)	Upper temperature threshold Select the upper temperature threshold (in °C). The MG90 will shut down if the internal temperature exceeds this threshold. 85.0 (Default) 73.0 60.0

Table G-2: General > Shutdown screen fields (Continued)

Field	Description
Low Temperature (°C)	Lower temperature threshold Select the lower temperature threshold (in °C). The MG90 will shut down if the internal temperature drops below this threshold. 0.0 -20.0 -30.0 (Default) -40.0
Uptime Extension After Ignition Off (hrs)	Time before shutdown after turning off ignition Enter the time, in hours, that the MG90 stays on and remains communicating after turning off the vehicle ignition. - Range: 0–25.5 0.0 (Default) <i>Note: Choose this time carefully. If too much time is specified, the vehicle's battery may be drained.</i>
Button Reset Time (secs)	Required duration for Reset button press Enter the amount of time (in seconds) that the Reset button must be pressed to trigger a factory reset. - Range: 0–255 10 (Default)

G.3 General > Services

The Device Service Configuration screen is used to configure event reporting.

The screenshot displays the 'Device Service Configuration' window within the MG90 software. The window has a title bar with tabs for 'Status', 'Devices', 'Security', 'LAN', 'WAN', 'GPS', 'General', 'Logs', 'Applications', and 'Logout'. Below the title bar, there are sub-tabs for 'Startup', 'Shutdown', 'Services', 'Tools', 'Backup/Restore', and 'Advanced Routing Rules'. The 'Services' tab is active, showing the 'Device Service Configuration' settings. The settings include:

- 'Use Automatic Event Server' checked.
- 'Alternate Event Server Address' with an empty text field.
- 'Enable Beacon Service' unchecked.
- 'WiFi Country Code' set to 'US (United States of America)'.
- 'Enable Network NTP' checked.
- 'Use Network NTP Default Servers' checked.
- 'Alternate Network NTP Servers' with an empty text area.
- 'Enable DNS Logging' checked.
- 'DNS Log Level' set to 'Warning'.

 At the bottom of the window are 'Save' and 'Cancel' buttons.

Figure G-3: LCI: General > Services—Sample screen

Table G-3: General > Services screen fields

Field	Description
Recommendation: The following settings (shaded rows) should only be modified as directed by Sierra Wireless.	
Use Automatic Event Server	Enable / disable a default event server - Selected — Use the default event server (<ESN>.dels.omgservice.com) that was set up for the MG90 by Sierra Wireless, where <ESN> is the MG90's serial number. (Default) - Not selected — Use the specified Alternate Event Server Address
Alternate Event Server Address	Enter the address of the event server to be used. <i>Note: This field is available only if Use Automatic Event Server is not selected.</i>
Enable Beacon Service	Send WAN status signal to the LAN to allow LAN clients to know if the WAN connection is up or down. - Selected — Enabled. Send UDP "1" (up) or "0" (down) to the LAN to indicate WAN status - Not selected — Disabled. No status signal is sent. <i>Note: This is a legacy feature. The Status Broadcast feature (Status > Broadcast) is recommended since it provides more complete status information. See Broadcast Router Status on page 28 for details.</i>
Wi-Fi Country Code	Wi-Fi country code Select the country code that the MG90 will broadcast.
<i>Note: Use the following fields to specify your NTP server configuration.</i>	
Enable Network NTP	Enable / disable network NTP - Selected — Enabled (Default) - Not selected — Disabled
Use Network NTP Default Servers	NTP servers to be used - Selected — (Default) Use the network NTP default servers Default servers are: 0.north-america.pool.ntp.org 1.north-america.pool.ntp.org 2.north-america.pool.ntp.org - Not selected — Use the servers in the Alternate Network NTP Servers (next field) list.
Alternate Network NTP Servers	Enter the alternate network NTP servers (FQDNs or IP addresses) that will be used instead of the default servers. (This is typically used in a closed (private) network instead of the public Internet.) Enter one server per line. For example: 0.usernetwork.org 1.usernetwork.org 2.usernetwork.org <i>Note: This field is available only if Use Network NTP Default Servers is not selected.</i>

Table G-3: General > Services screen fields (Continued)

Field	Description
Enable DNS Logging	Enable/disable DNS logging - Selected — Enabled (Default) - Not selected — Disabled
DNS Log Level	Select the lowest severity level of DNS logs to save. Note that the lower the selected severity level, the more logs are saved. For example, selecting "Info" level logs will save Info, Notice, Warning, Error and Critical level logs. - Critical — Save only critical logs - Error - Warning — Save warning, error, and critical logs - Notice — Save notice, warning, etc. logs - Info - Debug Level 1 - Debug Level 2 - Debug Level 3 - Debug Level 4 - Debug Level 5 — Save all logs (Debug Level 5 to Critical)

G.4 General > Tools

The MG90 is equipped with a suite of diagnostic and device management 'command line' tools. The Tools tab allows you to choose the tools to run and enter their required command line arguments.

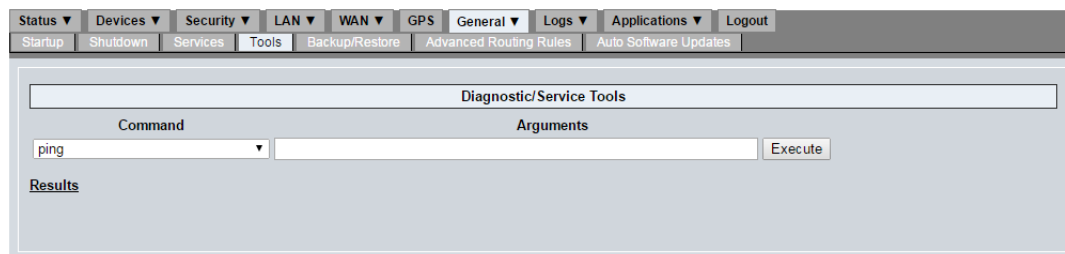


Figure G-4: LCI: General > Tools—Sample screen

Table G-4: General > Tools screen fields

Field	Description
Command	Select a diagnostic/service command, and then enter appropriate arguments and click Execute to run the command: - ping—Send an ICMP ping to network hosts. Can be used to determine if a particular host is reachable by the MG90. - dhcp-leases—Display the current DHCP leases assigned by the LAN Segment DHCP server. - tracert—UNIX traceroute utility. Display a list of all gateways between the MG90 and the specified host. - route—Display the MG90's current routing table. - arp—Display the MG90's cached mappings between IP addresses and MAC addresses. - netstat—Display network connections, routing tables, interface statistics, masquerade connections and multicast memberships. - ifconfig—Display the configuration for each network interface. - iwconfig—Display the configuration of each wireless interface. - iwlist—Display additional information from a wireless network interface that is not displayed by iwconfig. The main argument is used to select a category of information while iwlist displays all detailed information related to this category, including information already shown by iwconfig. - ipsec-vpn-status—Display the output from the IPsec status command which shows statistics regarding your current IPsec VPN connection. - dig—Domain Information Groper. Query DNS name servers to troubleshoot DNS issues, perform DNS lookups, etc. - nslookup—Query DNS name servers to get domain name or IP address mapping. - clean-local-software-update-cache—Clear the local cache. - verify-local-software-repository—Check for possible local storage organizational problems. - download-new-software-updates—Manually download new software updates. - enable-fips-cryptographic-modules—Enable FIPS mode of operation on the MG90 (this option is only available on devices where FIPS is not already enabled). <i>Note: Be careful when enabling FIPS, as there is no option to revert from FIPS to non-FIPS.</i> - reboot-device—Reboot the MG90. - lsusb—Display information about the USB buses available and the devices currently connected to them. - enable-usb-bypass-PEM-CA—Allow a PC to directly access the Cellular A module via USB port B (the lower port on the rear panel). This could be used to allow a PC application (for example, Sierra Wireless' Skylight) to establish a network connection using the Cellular A module. - enable-usb-bypass-PEM-CB—Same as enable-usb-bypass-PEM-CA, but for the Cellular B module. - disable-usb-bypass—Stop the Cellular A or Cellular B bypass. - dmccapture—Capture the cellular chip's diagnostic log. - trigger-prl-update—Update the preferred roaming list if an update is available. - update-data-profile—Force cellular module to update data profile with carrier. - factory-reset-module—Force a factory reset of a cellular module.
Arguments	Command arguments Enter appropriate arguments for the selected command.
Execute (button)	Click to execute the selected command and show the command output in Results.
Results	Output of selected command

G.5 General > Backup/Restore

The Backup/Restore tab is used to:

- Back up the MG90's configuration (multiple backups can be saved), and if required, restore a saved configuration.
- Reset the MG90's configuration completely to factory default settings, or to reset all except selected 'core' settings.

Figure G-5: LCI: General > Backup/Restore—Sample screen

Table G-5: General > Backup/Restore screen fields

Field	Description
Backup/Restore Configuration	
Backup configuration	Click backup to save the current MG90 configuration as a gzip file (config-<date>.tar.gz) in your default downloads folder.
Restore Configuration	Click Choose File / Browse and navigate to the folder containing the configuration file you want to restore (config-<date>.tar.gz).
Restore (button)	Click Restore to reconfigure the MG90 with the selected configuration file.
Restore Results	When the restoration is complete, comprehensive details appear in the Restore Results section.
Reset Device Configuration	
Reset Mode	Choose which core settings (if any) will be retained when resetting the MG90 to factory defaults. ▪ Preserve the Core Settings (below) — All three types of core settings will be retained. The checkboxes are all automatically selected and cannot be changed. ▪ Preserve Selected Core Settings (below) — Select any/all of the checkboxes indicating the types of core settings to be retained. ▪ Reset All to Factory Defaults — All settings will be reset. The checkboxes are all automatically deselected and cannot be changed.
Preserve User Accounts and Passwords used to Access this Device	▪ Selected — User accounts and passwords will be retained during a factory reset. ▪ Not selected — All user accounts are removed during a factory reset.

Table G-5: General > Backup/Restore screen fields (Continued)

Field	Description
Preserve Client Certificates / Credentials used to Access Organization's Intranet	- Selected — All client certificates and credentials for the Intranet will be retained during a factory reset. - Not selected — All client certificates and credentials for the Intranet are removed during a factory reset.
Preserve Client Certificates / Credentials used with Management System	<i>Note: Field is reserved for future use and cannot be changed manually.</i>
Execute Reset (button)	Click Execute Reset to reset the MG90 to factory defaults except for selected core settings.

G.6 General > Advanced Routing Rules

Advanced routing rules are custom scripts that can be executed at boot time, on WAN link activation, on LAN activation, or when a WAN connection changes from connected to disconnected.

Important: *These scripts should only be used under direction of Sierra Wireless Technical Support.*

Important: *The system supports the use of either advanced routing rules or policy based routing rules, but not both. If setting up advanced routing rules, make sure to remove any existing policy based routing rules ([Policy-Based Routing Rules](#) on page 226).*

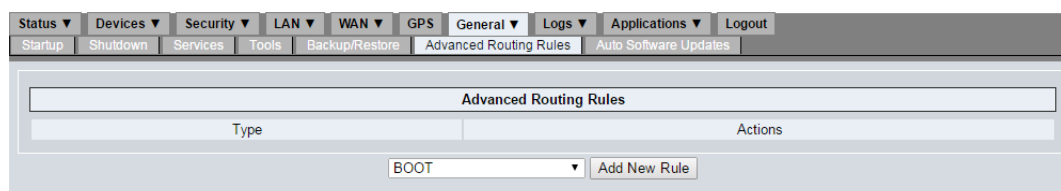


Figure G-6: LCI: General > Advanced Routing Rules—Sample screen

Table G-6: General > Advanced Routing Rules screen fields

Field	Description
Type	Script type: - BOOT — a boot file executes once on system boot. - LAN-Activation — this type of file executes after a bridge interface is brought up. The script argument uses the bridge name (e.g. br0). - WAN-Device State Change — this routing rule executes when a link changes state, for example from UP to DOWN and vice versa. Inputs include the interface IP address and the gateway IP address. - WAN-Activation — this file executes when a link becomes the active link. Inputs include the interface IP address and the gateway IP address.
Actions	Click these optional links to perform actions on the associated scripts: - Delete — Delete the associated script. - Configure — Configure the associated script. See General > Advanced Routing Rules > Add New Rule/Configure Rule on page 246.
Add New Rule (button)	Select the script type to add and click Add New Rule: - BOOT — Boot file that executes once on system boot. - LAN-Activation — Executes after a bridge interface is brought up. The script argument uses the bridge name (e.g. br0). - WAN-Device State Change — Routing rule that executes when a link changes state, for example from UP to DOWN and vice versa. Inputs include the interface IP address and the gateway IP address. - WAN-Activation — Executes when a link becomes the active link. Inputs include the interface IP address and the gateway IP address.

G.6.1 General > Advanced Routing Rules > Add New Rule/Configure Rule

The Advanced Routing Rules screen is used to enter a custom script of the type that you selected in General > Advanced Routing Rules.

Figure G-7: LCI: General > Advanced Routing Rules > Add New Rule/Configure Rule—Sample screen

Table G-7: General > Advanced Routing Rules > Add New Rule (or Configure) screen fields

Field	Description
Type	Script type and description of when the script will execute
Description	- BOOT — Boot file that executes once on system boot. - LAN-Activation — Executes after a bridge interface is brought up. The script argument uses the bridge name (e.g. br0). - WAN-Device State Change — Routing rule that executes when a link changes state, for example from UP to DOWN and vice versa. Inputs include the interface IP address and the gateway IP address. - WAN-Activation — Executes when a link becomes the active link. Inputs include the interface IP address and the gateway IP address.
Script entry box	Enter the required script (series of commands)

G.7 General > Auto Software Updates

The Auto Software Updates tab is used to:

- Configure how software updates are downloaded and installed.
- Configure firmware switching and image management.

The screenshot shows the 'Automatic Software Update Configuration' screen. It has a top navigation bar with tabs: Status, Devices, Security, LAN, WAN, GPS, General (selected), Logs, Applications, and Logout. Below this is a sub-navigation bar with: Startup, Shutdown, Services, Tools, Backup/Restore, Advanced Routing Rules, and Auto Software Updates (selected).

The main content area is titled 'Automatic Software Update Configuration' and contains several sections:

- Options:**
 - Enabled: ☒
 - Allow Downgrade: ☐
 - Upgrade Options:
 - ☐ Download Updates Only
 - ☒ Download and Apply Updates on Next Boot
 - ☐ Download and Apply Updates during Scheduled Time (UTC time without DST)
 - Download Bandwidth Limit (KB/s):
 - Download Timeout (Seconds):
 - Download on High Cost Link: ☐
- Radio Module Firmware Options:**
 - Firmware Upgrade Option:
 - Firmware Upgrade on High Cost Link: ☐
 - SIM-based Switching Enabled on CA: ☒
 - SIM-based Switching Enabled on CB: ☒
- Radio Module Firmware Available:** A table showing available firmware updates.

Active	Status	Module	Carrier	Firmware Version	Size (MB)	Upgrade Disabled	Force Firmware	Purge
CA	Available	MC7354	GENERIC	SWI9X15C_05.05.58.00_Generic_005.025_002	35	☐	None	Never
CB	Available	MC7455	GENERIC	SWI9X30C_02.30.03.00_GENERIC_002.046_001	65	☐	None	Never
- Add Firmware:**
 - Remaining Disk Space (MB): 190
 - EM7511 ATT
 - Choose and Upload a File From Your Computer
- Radio Module Current Status:**
 - Cellular CA
 - RM: MC7455
 - SIM: GENERIC
 - SIM ICCID: 8933240467726677726
 - SIM IMSI: 222094589795795
 - Firmware: 02.30.03.00_GENERIC_002.046_001
 - SKU PRI: 9904514
 - Carrier PRI: 9999999_9904609_SWI9X30C_02.30.03.00_GENERIC_002.046_001

At the bottom are 'Submit' and 'Cancel' buttons.

Figure G-8: LCI: General > Auto Software Updates—Sample screen

Table G-8: General > Auto Software Updates screen fields

Field	Description
Options The following options control MG90 firmware updates.	
Enabled	Enable/disable automatic software updates - Selected — Enabled (Default). The MG90 will check for any update(s) that have been published to AMM and automatically download and apply them based on the selected Upgrade Options. - Not selected — Disabled.
Allow Downgrade	Enable installation of software downgrades - Selected — Enabled. Software versions lower than that currently installed can be downloaded and applied as well as upgrades. - Not selected — Disabled (Default). Only higher versions can be downloaded and applied.
Upgrade Options	- Download Updates Only — The MG90 does not automatically apply any updates that have been downloaded. To apply updates, select one of the other two options. The updates will then be applied based on the rules for those selections. - Download and Apply Updates on Next Boot — (Default) When the MG90 boots, it automatically applies any updates that have been downloaded. - Download and Apply Updates during Scheduled Time (UTC time without DST) — If any updates have been downloaded, the MG90 applies them during the 'scheduled time': - Attempt Upgrade — How often upgrades can be installed: - Just Once — Only on the scheduled date and time slot - Every Day — Each day beginning on Start From - Every Week — Once per week beginning on Start From (e.g. 17 May 2017 is weekly attempts on Wednesdays) - Every Month — Once per month beginning on Start From (e.g. 17 May 2017 is monthly attempts on the 17th) - Start From — First day that updates can be applied. If date is last day of the month, 'every month' upgrades will be on the last day of each month. - Between — Time slot (UTC times) during which updates can be applied. (DST adjustments are not applied to the time slot.) <i>Note: In cases where the unit is never shut off (i.e. when a vehicle is in operation 24 hours per day, 7 days per week), use the 'Scheduled Time' upgrade option to install updates.</i>
Disable Boot Checks on Ignition Shutdown	Disable/enable automatic checks for software updates when the MG90 reboots after a clean shutdown that occurred due to turning off the vehicle ignition. - Selected — The MG90 will not automatically check for software updates when it reboots. - Not selected — (Default) The MG90 automatically checks for software upgrades, regardless of the reason it shut down and rebooted.
Download Bandwidth Limit (KB/s)	Bandwidth available for downloading software updates Set the maximum bandwidth (in KB/s) available for downloading updates over the WAN link. This can be used to ensure that adequate bandwidth is available for regular communications over the WAN.
Download Timeout (Seconds)	Download timeout period Enter the amount of time (in seconds) after which failure to receive data causes the download to time out. The download will stop, and then continue when the gateway comes back online. This field is useful for slower links that may require larger values when dealing with large files, or when dealing with a bad link that frequently jumps between being offline and online. Default: 600

Table G-8: General > Auto Software Updates screen fields (Continued)

Field	Description
Download on High Cost Link	Enable/disable software download on high cost WAN links - Selected — Enabled. The MG90 will download the update even when a high-cost WAN link is in use (e.g. a cellular connection). - Not selected — Disabled (Default). The MG90 downloads updates only on low-cost WAN links (e.g. Wi-Fi access point within a vehicle depot). This also disables the Firmware Upgrade on High Cost Link field. <i>Tip: If bandwidth consumption is a concern (e.g. due to cost), set the cellular link to be a high cost link, and disable the Download on High Cost Link option.</i>
Radio Module Firmware Options The following options control carrier-specific firmware image updates for the MG90's on-board MC7354/MC7430/MC7455/EM7511/EM7565/EM9190 cellular WAN modules:	
Firmware Upgrade Option	Enable/disable automatic firmware downloading If enabled (Upgrade Active or Upgrade All), the MG90 automatically downloads and upgrades firmware images as described below: - Upgrade Active (Default) — Download and upgrade the Available firmware images that are in the Radio Module Firmware Available list only if they are also currently running on cellular modules. <i>Important: Selecting "Upgrade Active" clears the Upgrade Disabled checkbox for the active images. If this is selected accidentally, make sure to click Cancel (or change screens without clicking Submit) so none of the changes are saved.</i> - Upgrade All — Download and upgrade all of the Available / Requested firmware images that are in the Radio Module Firmware Available list. <i>Important: Selecting "Upgrade All" clears the Radio Module Firmware Available list's "Upgrade Disabled" column and changes the "Purge" column values to "Never". If this is selected accidentally, make sure to click Cancel (or change screens without clicking Submit) so none of the changes are saved.</i> - Disabled — Firmware upgrade disabled (including the Add Firmware list and Add button) <i>Note: To prevent specific firmware images in the Radio Module Firmware Available List from being upgraded, select Upgrade Disabled.</i> <i>Note: The Firmware Upgrade Option is checked after an image switch occurs. If the value is "Upgrade Active", the Upgrade Disabled checkbox for the now-active firmware is automatically cleared.</i>
Firmware Upgrade on High Cost Link	Enable/disable firmware upgrades on high cost WAN links <i>Note: This field can be selected only if Download on High Cost Link is selected.</i> - Selected — Enabled. The MG90 will download the firmware image even when a high-cost WAN link is in use (e.g. a cellular connection). - Not selected — Disabled (Default). The MG90 downloads firmware images only on low-cost WAN links (e.g. Wi-Fi access point within a vehicle depot). <i>Note: If bandwidth consumption is a concern (e.g. due to cost), set the cellular link to be a high cost link, and disable the Firmware Upgrade on High Cost Link option.</i>

Table G-8: General > Auto Software Updates screen fields (Continued)

Field	Description
SIM-based Switching Enabled on CA	For the indicated cellular module (e.g. CA, CB), enable / disable carrier-based firmware image switching - Selected — Enabled (Default). The MG90 will detect the carrier based on the SIM card, and automatically install the appropriate image package for that carrier. <i>Note: When enabled, the router may require an additional 10 seconds (for each enabled option) to connect on boot. (e.g. 10 seconds if CA or CB is enabled, or 20 seconds if both are enabled)</i> <i>Note: The Force Firmware field for each module will be disabled.</i> - Not selected — Disabled.
SIM-based Switching Enabled on CB	
Radio Module Firmware Available List of firmware images currently stored on the MG90, upgrade / purge options, and tools to store additional images on the device.	
Active	For images that are also running on one or more cellular modules, indicates the module(s) (e.g. 'CA'; 'CB'; 'CA,CB')
Status	- Available — Firmware image is available for use. - Uploaded — Manually loaded on the MG90 via the Add Firmware 'To Upload' button. Image will not be upgraded via software upgrades. - Requested — Firmware has been selected using the Add Firmware list, and will be loaded on the device after it reboots.
Module	Module type (e.g. MC7455, EM9190, etc.) on which the firmware image can be loaded.
Carrier	Carrier (SIM provider) that the firmware can be used for.
Firmware Version	Firmware version number
Size (MB)	Amount of space the firmware takes up on the device's internal storage. <i>Note: The MG90 has 320 MB of storage for firmware images.</i>
Upgrade Disabled	If selected, prevents a newer version of the firmware from being loaded.
Force Firmware	- Cn — Force manual image switch on this cellular module. If selected, the firmware will be loaded on the module at the next boot. - Both — Force manual image switch on both cellular modules. If selected, the firmware will be loaded on both modules at the next boot. (This option appears only if there are two cellular modules.) - None — Default. Do not force a manual image switch. <i>Note: If SIM-based Switching Enabled on Cn is selected, Force Firmware is not available for the corresponding cellular module.</i>

Table G-8: General > Auto Software Updates screen fields (Continued)

Field	Description
Purge	Indicates under which conditions the firmware image can be purged when there is not enough space available for a required firmware update (e.g. when a SIM is switched) - If needed — The image can be purged automatically if a SIM-based switch is required and there is not enough space for the new image. Images are purged based on the priority sequence described in Purging Firmware Images on page 112. <i>Note: When If needed is selected, the Upgrade Disabled checkbox for the image is automatically selected, and cannot be changed.</i> - Now — Mark the image to be purged when Submit is clicked. For example, purge an image to make space for loading a new image using the Add Firmware list or To Upload button. <i>Note: When Now is selected, the Upgrade Disabled checkbox for the image is automatically selected, and cannot be changed.</i> - Never (Default) — Image cannot be purged automatically. <i>Note: When Never is selected, the Upgrade Disabled checkbox for the image remains selected and becomes accessible (can be changed). Make sure to de-select the checkbox if upgrades should be allowed for the image.</i>
Add Firmware	
Remaining Disk Space (MB)	Amount of space remaining on the MG90 to add images to the Radio Module Firmware Available list. (Maximum space available is 320 MB.)
Add Firmware pulldown list	Firmware images (for supported cellular modules) that are available for installation from AMM. - Select an image and click Add to add the item as 'Requested' in the Radio Module Firmware Available list. - Wait until a prompt indicates that the file has been downloaded to the MG90. - Reboot the MG90 to install the image. <i>Note: If the MG90 is rebooted before the file finishes downloading, it will automatically begin downloading again and will install after the next reboot.</i>
To Upload	Option to allow non-standard firmware images to be loaded from the computer. (e.g. a custom-built firmware from your company, or a firmware downloaded from source.sierrawireless.com) To add a firmware image, see Loading a signed image from Computer on page 106.
Radio Module Current Status	
SIM and firmware information for each Cellular module	
<i>Note: SIM and firmware information appears only if the module is not set to IDLE.</i>	
RM	Model (e.g. MC7455, EM9190, etc.) of the installed cellular module
SIM	SIM operator / carrier (e.g. GENERIC, AT&T, VERIZON, etc.)
SIM ICCID	SIM's unique ICCID (Integrated Circuit Card ID)
SIM IMSI	SIM's unique IMSI (International Mobile Subscriber Identity)
Firmware	Firmware version running on the cellular module.
SKU PRI	SKU-specific configuration (provisioning) version number
Carrier PRI	Carrier-specific configuration (provisioning) version number

H: Logs Tab

This chapter describes the Logs tab screens, which allow you to view system log (error /status) messages.

The Logs tab includes the following sub-tabs:

- Current Logs — Display logs that have not been uploaded to AMM. See [Logs > Current Logs](#) on page 252.
- Archived Logs — Display logs that have been uploaded to AMM. See [Logs > Archived Logs](#) on page 252.

H.1 Logs > Current Logs

The Current Logs tab lists all logs currently stored on the MG90 that will be uploaded to AMM at the end of the day.

FileName	Last Modified	Size
2016-07-07acetech.log	07-Jul-2016 14:58	14.7K
2016-07-07batchlogger.log	07-Jul-2016 15:01	15.8K
2016-07-07bluetoothservice.log	07-Jul-2016 05:44	6.4K
2016-07-07critical.log	07-Jul-2016 08:03	7.6K
2016-07-07dbcheckpointd.log	07-Jul-2016 15:08	89.7K
2016-07-07dbcleand.log	07-Jul-2016 15:08	11.0K
2016-07-07devices.log	07-Jul-2016 14:55	157.2K
2016-07-07dunappl.log	07-Jul-2016 05:44	4.5K
2016-07-07event.log	07-Jul-2016 00:50	0
2016-07-07firewall.log	07-Jul-2016 15:08	302.2K
2016-07-07firewall.log.1	07-Jul-2016 13:40	1.0M
2016-07-07firewall.log.2	07-Jul-2016 09:55	1.0M

Figure H-1: LCI: Logs > Current Logs—Sample screen

Table H-1: Logs > Current Logs screen fields

Field	Description
FileName	Log name comprising the date it was created and the feature the log applies to.
Last Modified	Date and time the log was last updated.
Size	File size in KB.

H.2 Logs > Archived Logs

The Archived Logs tab lists the logs that have been uploaded to AMM.

FileName	Last Modified	Size
2016-06-10acetech.log.zip	14-Jun-2016 22:30	730
2016-06-10bluetoothservice.log.zip	14-Jun-2016 22:30	779
2016-06-10critical.log.zip	14-Jun-2016 22:30	364
2016-06-10dbcheckpointd.log.zip	14-Jun-2016 22:30	569
2016-06-10dbcleand.log.zip	14-Jun-2016 22:30	466
2016-06-10devices.log.zip	14-Jun-2016 22:30	1.6K
2016-06-10dunappl.log.zip	14-Jun-2016 22:30	577
2016-06-10event.log.zip	14-Jun-2016 22:30	188
2016-06-10firewall.log.zip	14-Jun-2016 22:30	1.2K
2016-06-10framework.log.zip	14-Jun-2016 22:30	2.6K

Figure H-2: LCI: Logs > Archived Logs—Sample screen

Table H-2: Logs > Archived Logs screen fields

Field	Description
FileName	Log name comprising the date it was created and the feature the log applies to.
Last Modified	Date and time the log was last updated.
Size	File size in KB.

I: Applications Tab

Several value added applications are available for the MG90 that enhance and extend the MG90's capabilities.

Examples of common applications include:

- General Purpose I/O Configuration — Configure the behavior of the MG90's available GPIOs.
- Telemetry — Monitors and reports information about key vehicle telemetry parameters such as speed, acceleration etc.
- GNX Companion — Configure the MG90 for use with a GNX AirLink Companion device.
- Asset Manager — Reports GPS locations of tracked assets to AMM.

Each application requires configuration on both the MG90 and AMM. Configuration settings are application specific and may include modifiable settings, status information or both. Documentation for each application and its configuration is available at source.sierrawireless.com.

Note: Contact your Sierra Wireless Account Manager or Channel Partner to inquire about Application Licensing options.

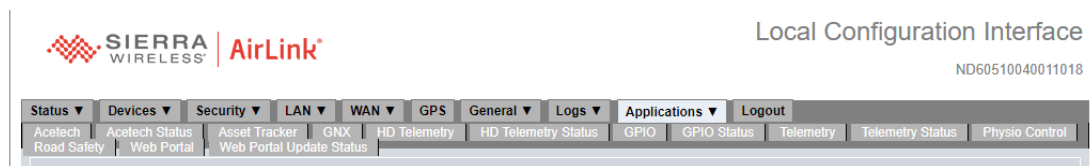


Figure I-1: Applications Tab

I.1 General Purpose I/O Configuration

The MG90 provides five GPIO (General Purpose I/O) signals that can be used to receive external sensor inputs or send data to external devices.

- Four GPIOs are provided on the DB9 serial connector
- One GPIO is provided on the power supply module.
- Each GPIO can be configured for Input or Output.

Note: Generic switch boxes can be used for GPIO testing.

This section describes the Applications GPIO tab, which allows you to configure the GPIOs.

Status ▾Devices ▾Security ▾LAN ▾WAN ▾GPS ▾General ▾Logs ▾Applications ▾Logout

AceTech AceTech Status Asset Tracker HD Telemetry HD Telemetry Status GPIO GPIO Status Telemetry Telemetry Status Physio Control Road Safety Web Portal Web Portal Update Status

General Purpose I/O Configuration

Options

Enable☒

Polling Period (seconds)

Default Severity

High ▾

Active State

High ▾

GPIO Pins/Report Configurations

GPIO	Pin	Enable Report	Input/Output	Severity	Active State
1	DB9-9	☒	Input ▾	Default ▾	Default ▾
2	DB9-4	☒	Output ▾	Default ▾	Low ▾
3	DB9-6	☒	Input ▾	Default ▾	Low ▾
4	DB9-1	☒	Output ▾	Default ▾	Default ▾
5	PSM-4	☒	Output ▾	Default ▾	Low ▾

Note: Please submit configuration changes before running test

Advanced GPIO Rules

This is a sample script with all the GPIO library functions
Note: All functionality is commented out

Get input states
db99 = GPIO.input(1)
db96 = GPIO.input(3)

Get network states
vpn = GPIO.getVPNStatus()
wanConn = GPIO.hasConnectedWan()
cellConn = GPIO.hasCellularConnection()
wifiConn = GPIO.hasWifiConnection()
ethConn = GPIO.hasEthernetConnection()

Get GPS state
gpsFix = GPIO.hasGpsData()

Set outputs
GPIO.output(2,1)
GPIO.output(4,1)

Run TestShow StatusStop TestDiscard ChangeClear Content

OUTPUT:

Test is Running...

Submit

Figure I-2: LCI: Applications > GPIO

I.1.1 Using GPIOs

This screen is used to configure the behavior of available GPIOs, and enter and store a script that can access the GPIOs and available GPIO API (library) functions.

Note: To view the past states of the available GPIOs, see [GPIO Status](#) on page 258.

To configure and use the GPIOs:

1. Select Enable to enable all GPIOs for use based on configuration settings on this screen.
2. Set a polling period measured in seconds. (e.g. if Polling Period is 0.1, all GPIOs are checked every 0.1 seconds)
3. Set a default DELS event severity level to be assigned to reportable events for any GPIO that is configured for Default severity.
4. Set the active state to be used for any GPIO that is configured for Default active state.

5. For each of the five available GPIOs:
 - a. Select Enable Report if DELS events on the GPIO are to be sent to AMM.
 - b. Select the GPIO direction (input to or output from the MG90).
 - c. Select a DELS severity level to assign to events on this GPIO. To use the Default Severity from the Options section, select Default.
 - d. Select the GPIO's active state (Low / High), or select Default to use the Active State from the Options section.
 - e. Click Submit to commit the GPIO configuration settings.
 - f. In the Advanced GPIO Rules editor pane, develop a script to process the GPIOs:
 - i. Enter (or paste from a text editor) a Python script to process GPIO inputs, outputs, and API function calls.
 - ii. While developing the script, use the editor buttons to test the script. (See [Table I-2](#) on page 257.)
 - iii. When the script is complete and ready to be stored and run on the MG90, click Submit.

Table I-1: Applications > GPIO screen fields

Field	Description
Options The following options are used to enable and set default details for all GPIOs.	
Enable	Enable / disable all GPIOs - Selected — Enabled (Default). GPIOs can be used as inputs or outputs depending on selected GPIO Pins/Report Configurations options. - Not selected — Disabled. GPIOs are not accessible. <i>Note: It is not possible to enable/disable individual GPIOs.</i>
Polling Period (seconds)	Interval between GPIO status checks, in seconds. Minimum recommended interval — 0.1 seconds (Default)
Default Severity	Default severity level assigned to DELS events (events that are forwarded to AMM) for GPIOs that have Severity (In the GPIO Pins/Report Configuration section) = Default
Active State	Active state of GPIOs that have Active State (in the GPIO Pins/Report Configuration section) = Default.
GPIO Pins/Report Configurations The following options define each available GPIOs direction, DELS event severity level, and active state.	
GPIO	GPIO number
Pin	Physical GPIO location - DB9-x — GPIO on DB9 connector, pin x - PSM-4 — GPIO on Power Supply Module, pin 4
Enable Report	Enable/disable DELS event reporting - Selected — Events (state change low→high or high→low) on this GPIO are reported to AMM. - Not selected — Events are not reported to AMM.
Input/Output	GPIO direction - Input - Output

Table I-1: Applications > GPIO screen fields (Continued)

Field	Description
Severity	Severity level assigned to DELS events for this GPIO If Default is selected, the Default Severity level in the Options section is used.
Active State	Active state of GPIO If Default, then Active State in the Options section is used.
Advanced GPIO Rules Script to process GPIO inputs/outputs, use GPIO APIs, etc.	
Rule editor pane	Text pane to enter Python script used to process GPIOs (read inputs, write outputs) and access GPIO API functions to determine various system conditions. The MG90 supports a single script only. To save additional scripts for later use, save them on a computer. When Submit is clicked, the script in the pane is written to the MG90, replacing the existing script (if one was previously saved).
OUTPUT	Output message area displaying results of testing the script.

Table I-2: GPIO Rule Editor Buttons

Button	Description
Run Test	Execute the script that is in the Rule Editor pane.
Show Status	Show the current status of all five GPIOs.
Stop Test	Stop executing the test.
Discard Changes	Remove all changes that have been made to the script since the last time Submit was clicked.
Clear Content	Clear the Rule editor.
Submit	Submit the script from the Rule editor to the MG90 to run in the background. The script will execute each time the gateway boots.

Table I-3: GPIO API Functions

API	Parameters	Return Value	Notes
GPIO.output(Port, State)	Port: 1–5 State: 0 1	void	Set state of specified output GPIO (1 is high) e.g. GPIO.output(4,1)
GPIO.input(Port)	Port: 1–5	0 1	Get state (1 is active high) of specified input GPIO e.g. GPIO.input(4)
GPIO.getVPNStatus()		Boolean	Returns true when VPN is connected
GPIO.hasConnectedWan()		Boolean	Returns true when WAN is connected
GPIO.hasCellularConnection()		Boolean	Returns true when there is a Cellular WAN connection
GPIO.hasWiFiConnection()		Boolean	Returns true when there is a Wi-Fi WAN connection

Table I-3: GPIO API Functions (Continued)

API	Parameters	Return Value	Notes
<code>GPIO.hasEthernetConnection()</code>		Boolean	Returns true when there is an Ethernet WAN connection
<code>GPIO.hasGpsData()</code>		Boolean	Returns true when GPS data is available
<code>GPIO.isWifiAccessPointEnabled()</code>		Boolean	Returns true when Wi-Fi Access Point is enabled

I.1.1.1 Sample GPIO Rule Script

The following script (shown in [Figure I-2](#) on page 255) demonstrates how each GPIO API can be used:

```
# This is a sample script with all the GPIO library functions
# Note: All functionality is commented out

# Get input states
# db99 = GPIO.input(1)
# db96 = GPIO.input(3)

# Get network states
# vpn = GPIO.getVPNStatus()
# wanConn = GPIO.hasConnectedWan()
# cellConn = GPIO.hasCellularConnection()
# wifiConn = GPIO.hasWifiConnection()
# ethConn = GPIO.hasEthernetConnection()

# Get GPS state
# gpsFix = GPIO.hasGpsData()

# Set outputs
GPIO.output(2,1)
# GPIO.output(4,1)
# GPIO.output(5,1)
```

I.1.2 GPIO Status

Displays the values of the GPIOs at each polling interval.

This section describes the Applications GPIO tab, which allows you to configure the GPIOs.

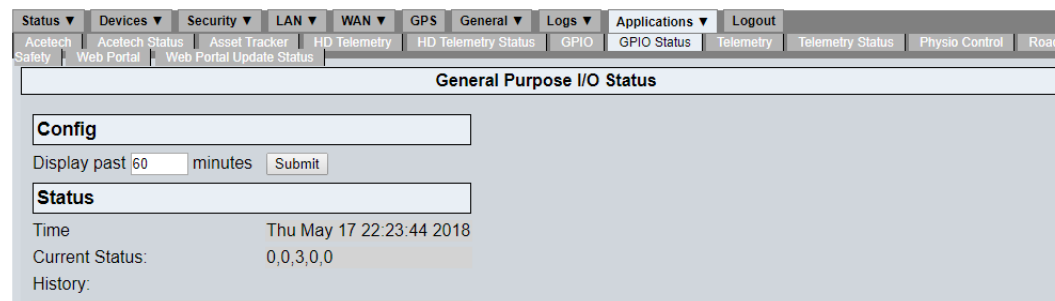


Figure I-3: LCI: Applications > GPIO Status

Table I-4: Applications > GPIO Status screen fields

Field	Description
Config Display options	
Display past <...> minutes	Number of minutes of GPIO state history (DELS events) to display No limit <i>Note: The MG90 cleans the events database on a regular basis. If the listing appears to be incomplete, check the event report on AMM, or the GPIO log on AMM or in the LCI (Logs > Current Logs).</i>
Submit (button)	Display all available GPIO state events recorded in the past number of minutes.
Status Current system time, most recent GPIO state, and GPIO state history	
Time	Current system time
Current Status	Most recent GPIO states - Format: <gpio_1_state>,<gpio_2_state>,<gpio_3_state>,<gpio_4_state>,<gpio_5_state> where <gpio_#_state> is 0 (low) or the gpio_# (high) - e.g. 0,0,3,0,0 indicates: - GPIO1 low - GPIO2 low - GPIO3 high - GPIO4 low - GPIO5 low
History	GPIO states reported in the past number of minutes.

I.2 Telemetry

The Telemetry and HD Telemetry applications (Telemetry, HD Telemetry, Telemetry Status and HD Telemetry Status) collect key telemetry data (speed, acceleration, etc.) from an OBD-II compliant scan tool connected to a vehicle's electronic interface system, and passes the data to AMM where it can be used to generate reports such as driver behavior, fuel consumption, and vehicle logistics.

Telemetry/Telemetry Status are used with light-duty vehicles, and HD Telemetry/HD Telemetry Status are used with heavy-duty vehicles.

OnBoard Diagnostic (OBDII) Configuration

Master Options

Enable ☐

Protocol

OBDII Adapter Attachment

- ☐ Use any serial port
- ☒ Use default rule, matches 0 attachments
- ☐ Restrict to position: Panel USB 1 - upper device
- ☐ Restrict to position: Panel USB 2 - lower device
- ☐ Restrict to position: Internal USB - primary device
- ☐ Restrict to position: Internal USB - secondary device

Mode 1 Bit-mapped PIDs

PID	Enabled	Description	Report When Bits Change By	Report When Value Stable For
\$01	☒	Monitor status since DTCs cleared	0xffffffff	0.0 s
\$03	☐	Fuel system status	0x0000001f	0.0 s
\$12	☐	Commanded secondary air status	0x00000007	0.0 s
\$1c	☐	OBD standards this vehicle conforms to	0x0000000f	0.0 s
\$41	☐	Monitor status this drive cycle	0xffffffff00	0.0 s

Mode 1 Numeric PIDs

PID	Enabled	Description	Report When Value Changes By	Report When Value Stable For
\$04	☐	Calculated engine load value	10.0 percent	0.0 s
\$05	☒	Engine coolant temperature	10.0 degrees C	900.0 s
\$06	☐	Short term fuel trim Bank 1	10.0 percent	0.0 s
\$07	☐	Long term fuel trim Bank 1	10.0 percent	0.0 s

Figure I-4: LCI: Applications > Telemetry

I.2.1 GNX Companion

The GNX Configuration screen is used to configure the MG90 to act as a connection gateway for a GNX AirLink Companion device, allowing the GNX device to use the MG90's WAN connection (via the MG90's GNX Companion Application) instead of its own modem or other external modems.

Note: The GNX must use the MG90's 'Serial LAN' LAN segment. This segment is only available when the MG90's Serial device is set to 'LAN'. (See [Configuring the Serial Port](#) on page 25.)

For setup details, see [Supporting Connection From GNX AirLink Companion Device](#) on page 72.

GNX Configuration

Enable ☒

LAN Segment

Server Host (IP)

Figure I-5: LCI: Applications > GNX

Table I-5: Applications > GNX screen fields

Field	Description
Enable	Enable / disable GNX AirLink Companion support - Selected — Enabled. Attached GNX device can use the MG90's WAN via the selected LAN Segment. - Not selected — Disabled. Attached GNX device cannot use the MG90's WAN.

Table I-5: Applications > GNX screen fields (Continued)

Field	Description
LAN Segment	LAN segment over which GNX device traffic is routed. ▪ This must be a Serial LAN device. Other segments will not work with the GNX device. (To create the Serial LAN segment, see Configuring the Serial Port on page 25.)
Server Host (IP)	IP address of the GNX Config Server. (For configuration details, refer to the GenX Reference Guide ([2] Gen-X Mobile Tracker — GNX20/6/5P/3 Legacy 10L/10 Command Reference and Parameter Definitions).

J: Logout Tab

Click the Logout tab to end your LCI session.

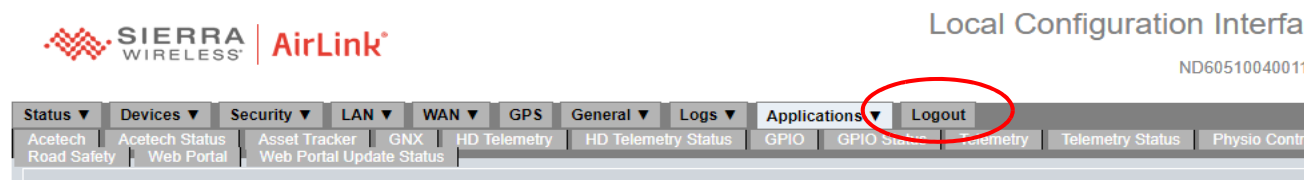


Figure J-1: Logout Tab

K: LEDs

The MG90 uses six LEDs to indicate its current operational status. The table below describes the behavior for each LED.

K.1 LED Behavior

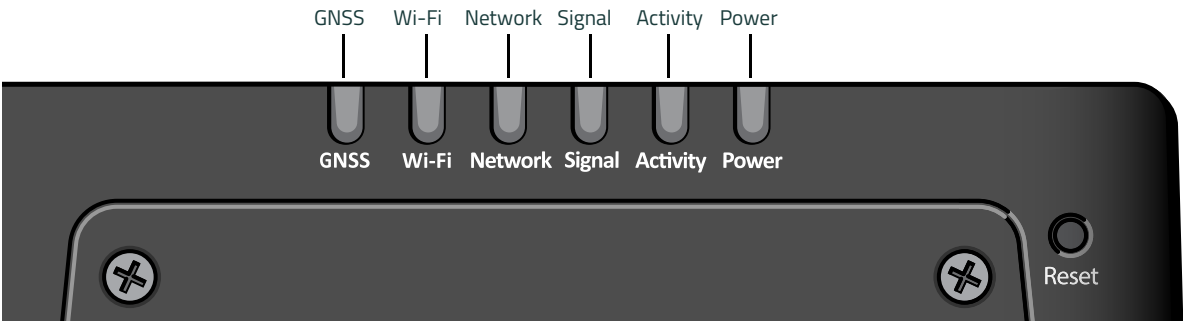


Figure K-1: MG90 LED Status Indicators (front panel)

Table K-1: LED Behavior

LED	Color / Pattern	Description
GNSS	Solid Green	Satellite fix is available, and Dead Reckoning is inactive (disabled, or not calibrated)
	Solid Blue	Satellite fix available, and Dead Reckoning is active
	Flashing Blue	No satellite fix is available, and Dead Reckoning is active
	Flashing Amber	No satellite fix is available, and Dead Reckoning is inactive (disabled, or not calibrated)
	Off	GNSS is off / disabled
Wi-Fi	Solid Green	Wi-Fi enabled (any mode), and not connected to an access point
	Flashing Green	Transmitting/receiving over Wi-Fi while not connected to an access point
	Solid Amber	Wi-Fi connected to an access point (i.e. Network state is "Network Ready - Wi-Fi")
	Flashing Amber	Transmitting/receiving over Wi-Fi while connected to an access point
	Off	Wi-Fi is off
Network	Flashing Amber	Connecting to a network
	Flashing Green	Connected to WAN (over cellular, Wi-Fi, or Ethernet)
	Solid Green	Connected to VPN
	Off	No network connection

Table K-1: LED Behavior (Continued)

LED	Color / Pattern	Description
Signal	<i>Note: If the active WAN link is:</i> - Cellular—Signal shown is for the cellular radio for that link. - Other (Wi-Fi, Ethernet, etc.)—Signal shown is for the strongest cellular radio.	
	Solid Green	Good signal (≥ 85 dBm; equivalent to 4–5 bars)
	Solid Amber	Average signal (≥ -100 dBm, < -85 dB; equivalent to 2–3 bars)
	Red	Poor signal (< -100 dBm; equivalent to 1 bar)
Activity	Flashing Green	Transmitting/receiving over the WAN interface
	Off	No WAN activity
Power	Solid Green	Power is present, normal operation
	Flashing Green	Power is present, MG90 is booting
	Solid Amber	Standby mode
	Flashing Red	- Slow blink (1 per second) — Temperature out of operating range - Fast blink (4 per second) — Voltage out of operating range
	Off	No power
ALL LEDS <i>Note: A 'chase' is all LEDS blinking in sequence.</i>	Green LED chase	Cellular module update or GNSS firmware update is in progress
	Purple LED chase	Software update is in progress
	Amber LED chase	
	Blue LED chase	MCU firmware update is in progress
	Solid White	Factory default reset is in progress When the factory reset finishes, the MG90 will power off and, if AutoPower is enabled (LCI General > Startup tab), will reboot.

L: JSON Data

This chapter describes the JSON schema used to broadcast the MG90 router status, and provides an example broadcast. For usage details, see [Broadcast Router Status](#) on page 28.

L.1 Broadcast Router Status — JSON Schema

```
{
  "$schema": "http://json-schema.org/schema#",
  "title": "gatewayStateBeacon",
  "type": "object",
  "required": ["timestamp", "vehicleID"],
  "properties": {

    "timestamp": {
      "type": "object",
      "properties": {
        "date": {
          "type": "string"
        },
        "time": {
          "type": "string"
        }
      }
    },

    "vehicleID": {
      "type": "string"
    },

    "location": {
      "type": "object",
      "properties": {
        "latitude": {
          "type": "number"
        },
        "longitude": {
          "type": "number"
        }
      }
    },

    "gpInputStates": {
      "type": "array",
      "items": {
        "type": "number"
      }
    },

    "gpOutputStates": {
      "type": "array",
      "items": {
        "type": "number"
      }
    },

    "wanState": {
      "type": "array",
```

```
"items": {
  "type": "object",
  "properties": {
    "friendlyName": {
      "type": "string"
    },
    "networkType": {
      "type": "string"
    },
    "status": {
      "type": "number"
    },
    "active": {
      "type": "boolean"
    },
    "bandNo": {
      "type": "string"
    },
    "bandwidth": {
      "type": "number"
    },
    "signalStrength": {
      "type": "number"
    },
    "RSSI": {
      "type": "number"
    },
    "RSRP": {
      "type": "number"
    },
    "RSRQ": {
      "type": "number"
    },
    "SINR": {
      "type": "number"
    },
    "5GNRBandNo": {
      "type": "string"
    },
    "5GNRBandwidth": {
      "type": "number"
    },
    "5GNRRSRP": {
      "type": "number"
    },
    "5GNRRSRQ": {
      "type": "number"
    },
    "5GNRSINR": {
      "type": "number"
    }
  }
},
"gnssStatus": {
  "type": "object",
  "properties": {
    "fix": {
      "type": "boolean"
    },
    "numberSatellites": {
      "type": "number"
    }
  },
}
```

```

        "antennaConnected": {
            "type": "boolean"
        }
    },
    "vpnState": {
        "type": "array",
        "items": {
            "type": "object",
            "properties": {
                "friendlyName": {
                    "type": "string"
                },
                "status": {
                    "type": "number"
                }
            }
        }
    },
    "generalInformation": {
        "type": "object",
        "properties": {
            "ignitionOn": {
                "type": "boolean"
            },
            "mainBatteryVoltage": {
                "type": "number"
            },
            "internalTemperature": {
                "type": "number"
            }
        }
    }
}

```

L.2 Broadcast Router Status — Example Data

```

{
    "timestamp": {
        "date": "05182020",
        "time": "1603"
    },
    "version": "4.4.1",
    "vehicleID": "0012",
    "location": {
        "latitude": 49.172114,
        "longitude": -123.07013
    },
    "gpInputStates": [
        0,
        1,
        0,
        0,
        1
    ]
}

```

```
,
"gpOutputStates": [
  0,
  0,
  0,
  0,
  0
],
"wanState": [
  {
    "friendlyName": "Verizon",
    "networkType": "Cellular",
    "status": 1,
    "active": true,
    "bandNo": "7",
    "bandwidth": 20,
    "signalStrength": -70.3,
    "RSSI": -80,
    "RSRP": -12,
    "RSRQ": -13.7,
    "SINR": 0.6,
    "5GNRBandNo": "n66",
    "5GNRBandwidth": 10,
    "5GNRRSRP": -102.000000,
    "5GNRRSRQ": -11.000000,
    "5GNRSINR": 15.000000
  }
],
"gnssStatus": {
  "fix": true,
  "numberSatellites": 16,
  "antennaConnected": true
},
"vpnState": [
  {
    "friendlyName": "VPN #1",
    "status": 0
  },
  {
    "friendlyName": "Another VPN",
    "status": 1
  }
],
"generalInformation": {
  "ignitionOn": true,
  "mainBatteryVoltage": 11.8,
  "internalTemperature": 35.56
}
}
```

M: References

M.1 Web Site Support

Check source.sierrawireless.com for the latest Sierra Wireless product documentation.

M.2 Reference Documents

- [1] AirLink MG90 Hardware User Guide
Reference number: 4118699
- [2] Gen-X Mobile Tracker — GNX20/6/5P/3 Legacy 10L/10 Command Reference and Parameter Definitions
Reference number: 41111445
- [3] AirLink Mobility Manager Operation and Configuration Guide
Available at source.sierrawireless.com/resources/airlink/amm/omm-user-guides/
- [4] Certificate Management via AMM
Reference number: 41113515