ALEOS 4.4.9 Software Configuration

User Guide for AirLink ES440



SIERRA WIRELESS®

41113620
Rev. 1

Important Notice

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. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless product are used in a normal manner with a well-constructed network, the Sierra Wireless 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. Sierra Wireless accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the Sierra Wireless product, or for failure of the Sierra Wireless product to transmit or receive such data.

Safety and Hazards

Do not operate the Sierra Wireless product in areas where blasting is in progress, where explosive atmospheres may be present, near medical equipment, near life support equipment, or any equipment which may be susceptible to any form of radio interference. In such areas, the Sierra Wireless product **MUST BE POWERED OFF**. The Sierra Wireless product can transmit signals that could interfere with this equipment.

The driver or operator of any vehicle should not operate the Sierra Wireless product while in control of a vehicle. Doing so will detract from the driver or operator's control and operation of that vehicle. In some states and provinces, operating such communications devices while in control of a vehicle is an offence.

In accordance with ANSI/ISA 12.12.1-2011, Section 16 and CSA C22.2 No 213, Section 5.5, the following instructions and warnings apply:

This apparatus is suitable for use in Class I, Division 2, Groups A, B, C and D.

Warning: *EXPLOSION HAZARD–SUBSTITUTION OF COMPONENTS MAY IMPAIR SUITABILITY FOR CLASS I, DIVISION 2.*

Avertrissement: *RISQUE D'EXPLOSION-LA SUBSTITUTION DE COMPOSANTS PEUT RENDRE CE MATERIEL INACCEPTABLE POUR LES EMPLACEMENTS DE CLASSE I, DIVSION 2.*

Warning: *EXPLOSION HAZARD–DO NOT DISCONNECT WHILE CIRCUIT IS LIVE UNLESS THE AREA IS KNOWN TO BE NON-HAZARDOUS.*

Avertrissement: *RISQUE D'EXPLOSION-NE PAS DEBRANCHER TANT QUE LE CIRCUIT EST SOURS TENSION, A MOINES QU'IL NE S'AGISSE D'UN EMPLACEMENT NON DANGEREUX.*

Warning: *DO NOT USE THE USB CONNECTOR IN A HAZARDOUS AREA.*

Avertrissement: *NE PAS UTILISER DE CONNECTEUR USB DANS LES ENVIRONNEMENTS DANGEREUX.*

Limitation of Liability

The information in this manual is subject to change without notice and does not represent a commitment on the part of Sierra Wireless. SIERRA WIRELESS AND ITS AFFILIATES SPECIFICALLY DISCLAIM LIABILITY FOR ANY AND ALL DIRECT, INDIRECT, SPECIAL, GENERAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES INCLUDING, BUT NOT LIMITED TO, LOSS OF PROFITS OR REVENUE OR ANTICIPATED PROFITS OR REVENUE ARISING OUT OF THE USE OR INABILITY TO USE ANY SIERRA WIRELESS PRODUCT, EVEN IF SIERRA WIRELESS AND/OR ITS AFFILIATES HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR THEY ARE FORESEEABLE OR FOR CLAIMS BY ANY THIRD PARTY.

Notwithstanding the foregoing, in no event shall Sierra Wireless and/or its affiliates aggregate liability arising under or in connection with the Sierra Wireless product, regardless of the number of events, occurrences, or claims giving rise to liability, be in excess of the price paid by the purchaser for the Sierra Wireless product.

Patents

This product may contain technology developed by or for Sierra Wireless Inc. This product includes technology licensed from QUALCOMM®. This product is manufactured or sold by Sierra Wireless Inc. or its affiliates under one or more patents licensed from MMP Portfolio Licensing.

Copyright

© 2020 Sierra Wireless. All rights reserved.

Trademarks

Sierra Wireless®, AirLink®, AirVantage® and the Sierra Wireless logo are registered trademarks of Sierra Wireless.

Windows® and Windows Vista® are registered trademarks of Microsoft Corporation.

Macintosh® and Mac OS X® are registered trademarks of Apple Inc., registered in the U.S. and other countries.

QUALCOMM® is a registered trademark of QUALCOMM Incorporated. Used under license.

Other trademarks are the property of their respective owners.

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

Contents

Introduction 10

Overview 10

Sierra Wireless AirLink Products 10

About Documentation 10

Tools and Reference Documents 11

Gateway Configuration 12

Toolbar 13

Configuring your AirLink Gateway 13

Saving a Custom Configuration as a Template 14

Applying a Template 16

Update the ALEOS Software and Radio Module Firmware 18

Step 1—Planning Your Update 18

Recommendations 20

Step 2—Update the ALEOS Software and Radio Module Firmware 20

Updating Only the Radio Module Firmware 25

Enterprise LAN Management 26

Configuring Your Gateway for use in a PCI Compliant System 27

Status 29

Home 29

WAN/Cellular 35

LAN 39

VPN 42

Security 44

Services 45

Serial 46

Applications 48

About 49

WAN/Cellular Configuration 51
SIM PIN 61
Enable the SIM PIN 61
Change the SIM PIN 62
Disable the SIM PIN 63
Unblocking a SIM PIN 63
Re-Activation 64
Backup APN. 64
Bandwidth Throttle 65
Reliable Static Routing (RSR) 68
Dynamic Mobile Network Routing (DMNR) 72

LAN Configuration 79
Private and Public Mode 79
DHCP/Addressing 80
Ethernet 87
USB 90
Installing the USB Drivers 92
Host Port Routing. 94
Global DNS 96
PPPOE. 97
Configure the AirLink gateway to Support PPPoE 99
Configuring a PPPoE Connection in Windows 7 100
VLAN 103
VRRP 104
Host Interface Watchdog 108

VPN Configuration 110
Split Tunnel 110
IPsec Tunnel 111
GRE Tunnel 118
SSL Tunnel 119
VPN Failover 123

Security Configuration 126
Solicited vs. Unsolicited 126
Port Forwarding 126
DMZ 131
Port Filtering—Inbound 132
Port Filtering — Outbound 133
Trusted IPs—Inbound (Friends) 134
Trusted IPs—Outbound. 136
MAC Filtering 136

Services Configuration 138
AVMS (AirVantage Management Service). 138
ACEmanager 140
Dynamic DNS 142
Understanding Domain Names 147
Dynamic Names 148
SMS Overview 149
Sending SMS Commands to an AirLink Gateway 149
SMS Modes 150
Password Only 151
Control Only 152
Gateway Only 153
Control and Gateway 159
SMS Wakeup 160
SMS Security 162
Inbound SMS Messages 162
Trusted Phone Number 163
SMS Password Security 163
SMS > Advanced 165
SMSM2M 166
Telnet/SSH. 168
Email (SMTP). 169
Management (SNMP) 172

Time (SNTP) 177
Authentication 178
LDAP Authentication 178
RADIUS Authentication 180
TACACS+ Authentication 181
Device Status Screen 183

Events Reporting Configuration 184
Introduction 184
Configuring Events Reporting 185
Configuring Events Reporting 185
Email 185
SNMP TRAP 187
Report Data Group 187
Event Types 189

Serial Configuration 193
Port Configuration 193
Port Configuration 193
Reverse Telnet/SSH 196
Advanced 199
TCP 201
UDP 203
PPP/SLIP 205
Configuring IP to Serial with Auto Answer and Serial to IP 207
LED Indicator 211

Applications Configuration 212
Data Usage 212
ALEOS Application Framework 217

I/O Configuration 220
AirLink ES Series 220
Digital inputs 220
Relay outputs 221
Current State 221
Pulse Count 221
Configuration 222

Admin 224
Change Password 224
AAF User Password 225
Advanced 226
Radio Passthru 233
Log 234

Windows Dial-up Networking (DUN) 237
Installing a Device Driver 237
Creating a Dial-Up Networking (PPP) Connection 247

SNMP: Simple Network Management Protocol 257
Management Information Base (MIB) 257
SNMP Traps 257
Sierra Wireless MIB 257

AT Commands 282
AT Command Set Summary 282
Reference Tables 283
Device Updates 284
Status 285
WAN/Cellular 290
LAN 296
VPN 299
Security 304

Services 305
Serial 313
Standard (Hayes) commands 318
I/O 324
Applications 324
Admin 325

SMS Commands 328
SMS Command format 328
List of SMS Commands 329

Q & A and Troubleshooting 331
ACEmanager Web UI 331
Ethernet Ports 331
LAN Networks 331
Port Forwarding 331
ALEOS Application Framework (AAF) 332
SMS 332
VPN 333
Poor Wireless Network Connection 334
Connection not working 335
Updating the ALEOS Software and Radio Module Firmware 335
AirVantage Management Service 338
LTE Networks 339
SIM Card is Blocked 341
Remote connections 341
Radio Band Selection 342
Reliable Static Routing (RSR) 342
Inbound Ports Used by ALEOS 342
Event Reporting 343
TCP/IP and UDP/IP Auto Answer 343
Templates 345

Glossary of Terms 347

1: Introduction

Overview

ACEmanager™ is the free, web-based utility used to manage and configure the AirLink® device. It is a web application integrated in the ALEOS® software that runs on the AirLink gateway. AirLink Embedded Operating System (ALEOS) is purpose-built to maintain a wireless connection and to configure the gateway to the needs of the system. ACEmanager provides comprehensive configuration, monitoring, and control functionality to all AirLink gateways and routers.

ACEmanager enables you to:

- Login and configure device parameters
- Adjust network settings
- Change security settings
- Update events reporting and control outputs
- Update ALEOS software and radio module firmware
- Copy configuration settings to other AirLink gateways

Since ACEmanager can be accessed remotely over-the-air as well as locally, the many features of ALEOS can be managed from any location.

An ALEOS configuration template can be created using ACEmanager, after a single device is configured and installed, to program other AirLink gateways with the same configuration values. This enables quick, accurate deployment of large pools of devices.

Sierra Wireless AirLink Products

For more information on specific AirLink products, go to www.sierrawireless.com

About Documentation

Each chapter in the ALEOS Configuration User Guide describes a section (a tab in the user interface) of ACEmanager.

Chapters in this user guide explain:

- Parameter descriptions in ACEmanager
- Relevant configuration details
- User scenarios for certain sections in the guide.

Tools and Reference Documents

Document	Description
AirLink Gateway Hardware User Guide	This hardware document describes how to: • Install the AirLink gateway hardware • Connect the radio antennas • Connect a notebook computer and other input/output (I/O) devices • Interpret the LEDs and indicators on the AirLink gateway.
ALMS User Guide	AirLink Management Service features online help, videos and “How-To” pages that explain how to use ALMS for the remote management of Sierra Wireless AirLink gateways.

2: Gateway Configuration

To access ACEmanager:

1. Insert the SIM card, if applicable. Refer to the AirLink gateway hardware user guide for details.
2. Power on the AirLink gateway.
3. Launch your browser and enter the IP address and port number http://192.168.13.31:9191

   ACEmanager is supported on the latest versions of Internet Explorer® and Firefox®.

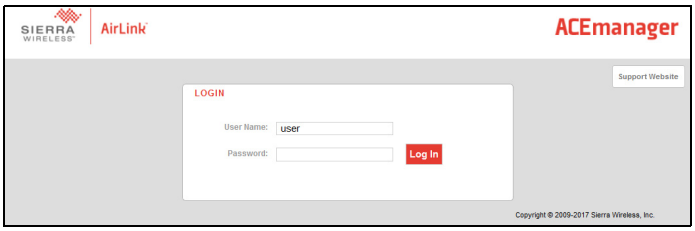


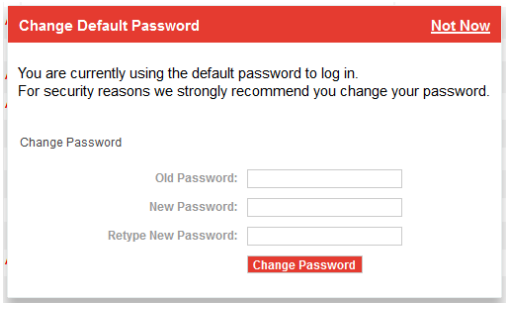
Figure 2-1: ACEmanager: Main Login screen

4. Log in:
   - User Name: “user” (entered by default)
   - Default Password: 12345

Note: ACEmanager has a default session idle timeout of 15 minutes. If there is no activity for the idle timeout period, you are redirected to the login screen. To change the session idle timeout period, see ACEmanager Session Idle Timeout (minutes) on page 141.

Note: For system security, ensure that you change the default ACEmanager password. The new password must be at least 8 characters long. For more information, see Change Password on page 224.

If your device is using the default password to log in to ACEmanager, a message to change the default password is displayed.



Note: By clicking “Not Now”, you may continue without changing the default password; however, you must accept the risk of bypassing this critical and strongly recommended security measure.

To prevent others from changing the AirLink gateway settings, you can change the ACEmanager password (see Change Password on page 224).

After your initial login to ACEmanager, you have the option of displaying the gateway status parameters on subsequent login screens.

1. In ACEmanager, go to Services > Device Status Screen.
2. In the Device Status on Login Screen field, select Enable. (For details, see Device Status Screen on page 183.)

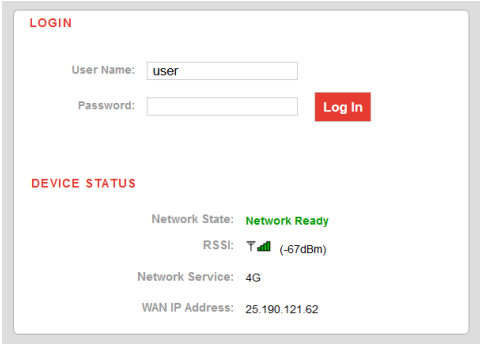


Figure 2-2: ACEmanager: Main Login screen with Device Status

Toolbar

The buttons on the ACEmanager toolbar are:

- Software and Firmware: Updates the ALEOS software and the radio module firmware
- Template:
  - Download and save a configuration as a template
  - Upload a saved template to apply settings
- Reboot: Reboots the gateway
- Refresh All: Refreshes all ACEmanager pages

Configuring your AirLink Gateway

There are three options for configuring the AirLink gateway:

- Use your browser-based ACEmanager (as detailed in this guide); or
- Use a terminal emulator application (e.g., Tera Term, PuTTY, etc.) to enter AT commands for many of the configuration options.
- Use the cloud-based AirVantage Management Service application (see www.sierrawireless.com/ALMS for more details.)

Saving a Custom Configuration as a Template

If you have a gateway configured to match your requirements, you can use ACEmanager to download and save that gateway's configuration as a template and then apply it to other Sierra Wireless AirLink gateways.

Note: Sierra Wireless recommends that templates be created and applied to AirLink gateways running the same version of ALEOS. If you apply a template created using an older version of ALEOS to a gateway running a newer version of ALEOS, settings for newly added features are not updated.

To download and save a custom configuration as a template:

1. Connect a laptop to the gateway with the configuration you want to save as a template.
2. In ACEmanager, click the Template button on the toolbar.

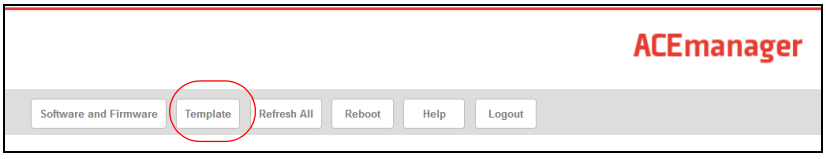


Figure 2-3: ACEmanager: Template button

The following window appears:

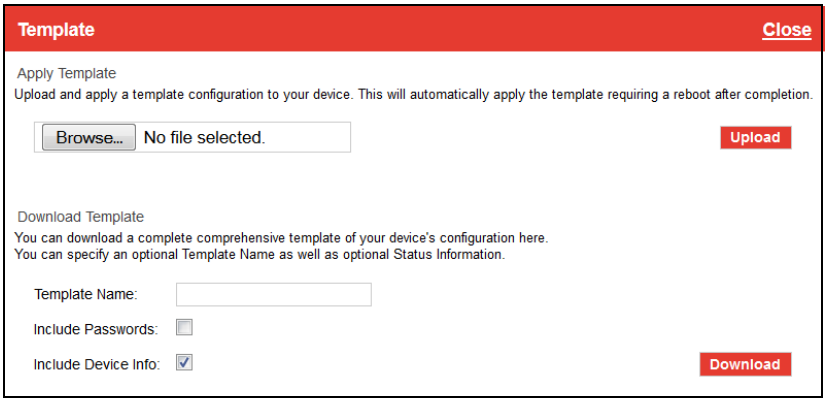


Figure 2-4: ACEmanager: Template window

Use the bottom half of the window to download and save a template.

3. If desired, enter a Template Name. The file is saved using this name and a.xml file extension. Spaces and special characters are not supported, and if entered, are deleted from the file name.

   If no Template name is entered, the file is saved as SWIApplyTemplate.xml.

4. Choose whether or not to:
   - **Include Passwords**
     When Include Passwords is selected, passwords configured in ACEmanager (such as the email password, the SMS ALEOS Command password, the Serial PPP password, etc.) are shown in plain text in the template file. When the template is

uploaded to a gateway, the passwords are included and replace any existing password configured on the gateway.
If Include Passwords is not selected, password fields are not included in the template file, and existing passwords persist when the template is uploaded to a gateway.

Note: The ACEmanager login password is not included when you select the Include Passwords option.

- **Include Device Info** (selected by default)
  When selected, the template file includes a "snap-shot" of the current Status tab information with the current settings. This could be useful for troubleshooting.

5. Click Download. The download status appears at the bottom of the window.

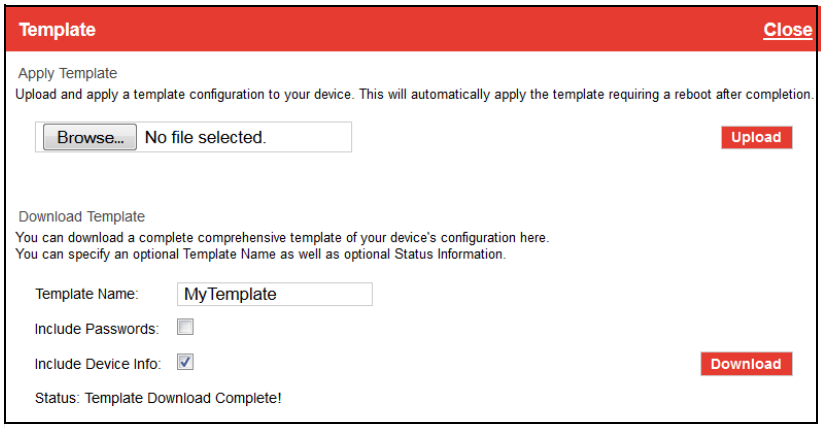


Figure 2-5: Download template complete

Once the download is complete, the following window opens:

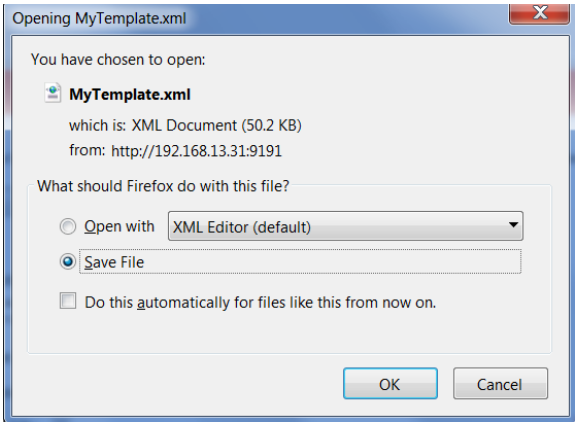


Figure 2-6: Open or Save the template file

6. In most cases, you will want to save the file to your computer for uploading to other AirLink gateways, but you also have the option to open the file.
   - Select Save File and click OK—file is saved to your computer (by default to the Downloads folder). If you entered a template name, the file is saved using that name. Otherwise, it is saved under the default name, SWIApplyTemplate.xml.

- Select Open and click OK—file opens in a text or XML editor as a human readable file. Use this option if you selected Include Device Info when you saved the file and want to view the device information (the text between the <devicestatus> and </devicestatus> tags is the snap-shot of the Device Info), or you want to compare this template with another template.

Warning: *Do not attempt to change settings directly in the template file. Changing settings in the template file could result in unexpected behavior in the AirLink gateway. Alter the template only if you are specifically directed to do so by your distributor or Sierra Wireless Technical Support.*

Tip: *If you want to compare a new template with the previous one, download and save the old template before applying the new one. You can use any 3rd party text comparison tool to check the differences between two templates.*

Applying a Template

Note: If you are using Internet Explorer 9 to upload the template, see Templates on page 345 for instructions on configuring the browser's Internet options to allow the upload.

To upload and apply a template to an AirLink gateway:

1. Connect the computer (where the template is saved) to the AirLink gateway you want to upload the template to.
2. In ACEmanager, click the Template button on the toolbar.

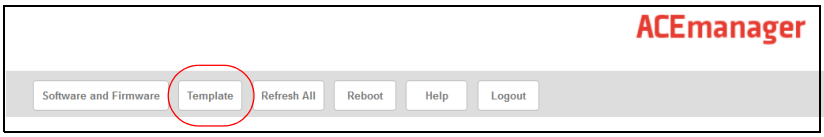


Figure 2-7: ACEmanager: Template button

The following window appears:

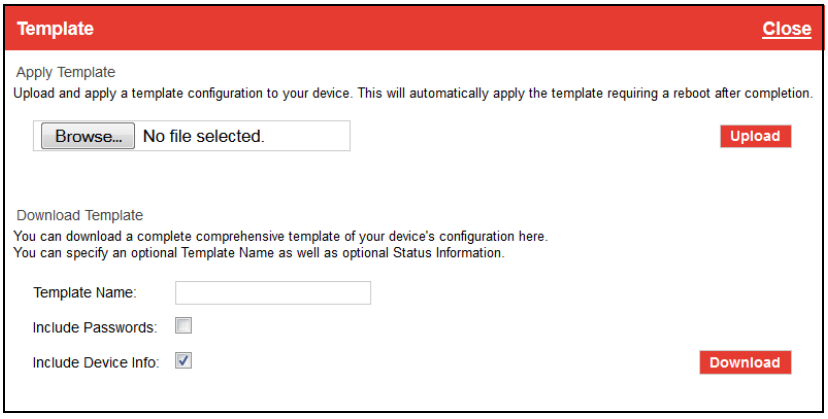


Figure 2-8: ACEmanager: Template window

Use the top half of the window to upload and apply a template to your AirLink gateway.

3. Click Browse... and navigate to the template you want to upload.
4. Click Open. The template file name appears beside the Browse... button.

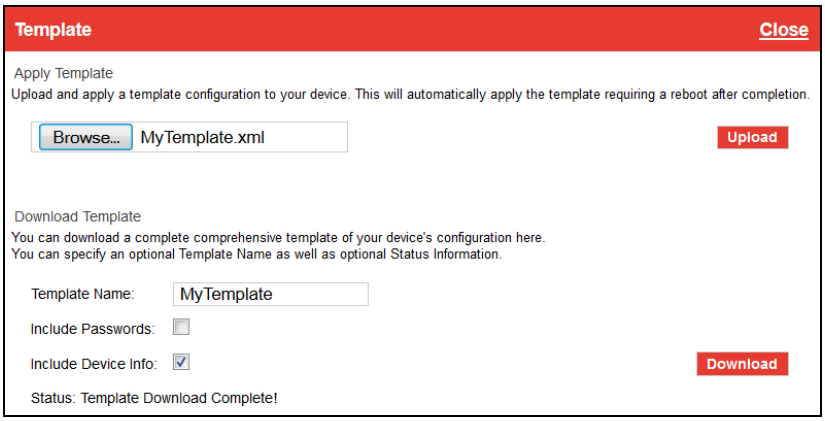


Figure 2-9: Apply Template file opened

5. Click Upload.
6. When the upload is complete, a Reboot button appears on the window.

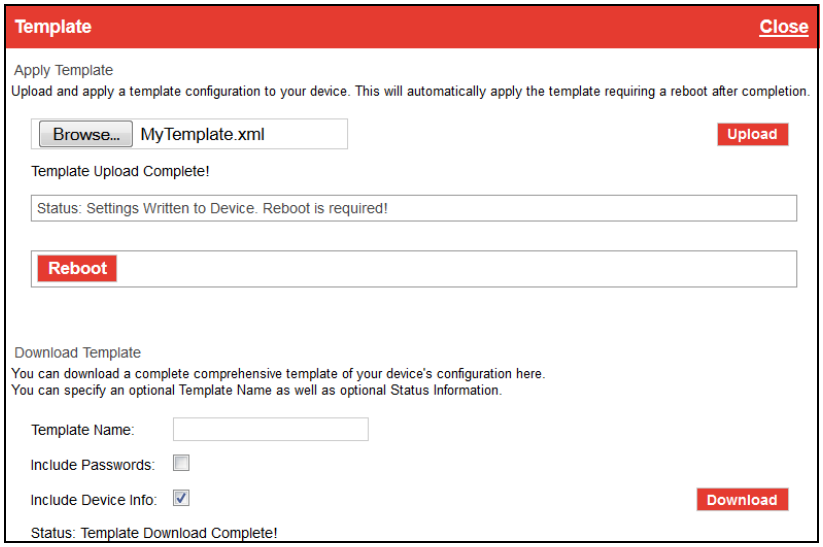


Figure 2-10: Template file uploaded

7. Click Reboot.
8. To confirm that the new template has been applied or to find out which template is currently on a gateway, go to Status > About and check the Template Name field.

Note: The Template Name field shows the last template applied and does not indicate any configuration changes made since the last template was applied.

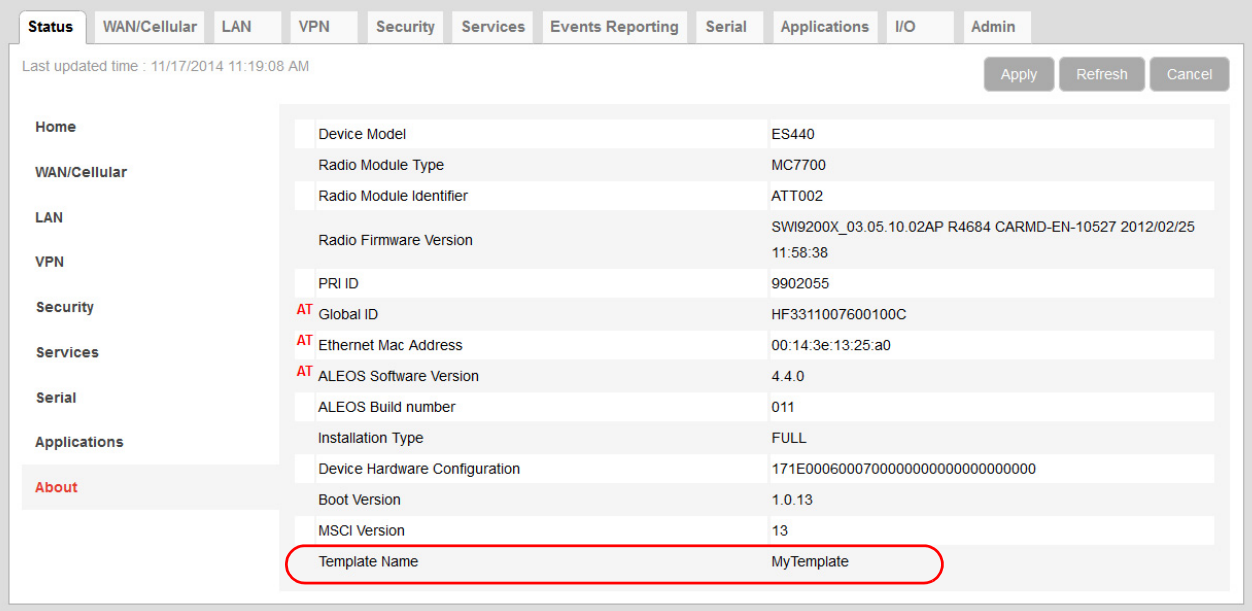


Figure 2-11: ACEmanager: Status > About

Note: If no template has been applied to the gateway since it was set or reset to the factory default settings, the template field is blank.

Update the ALEOS Software and Radio Module Firmware

To take advantage of new features available in the latest version of ALEOS, update the ALEOS software and radio module firmware on your AirLink gateways.

You can use ACEmanager to update one gateway at a time or AirVantage Management Service (AVMS) to update one or multiple gateways at the same time.

Step 1—Planning Your Update

Note: These instructions are for upgrading from ALEOS 4.3.6 or newer to 4.4.1. If you have an older version of ALEOS, refer to the Application Note: Updating from Older Versions of ALEOS.

1. Sierra Wireless recommends that you download a template from the gateway(s) before you begin the update process. For instructions, see Saving a Custom Configuration as a Template on page 14.
2. For each of the gateways you want to update, make a note of the:
   - Device Model
   - Radio Module Type
   - Radio Module Identifier
   - ALEOS Software Version

This information is available in AVMS and in ACEmanager (Status > About).

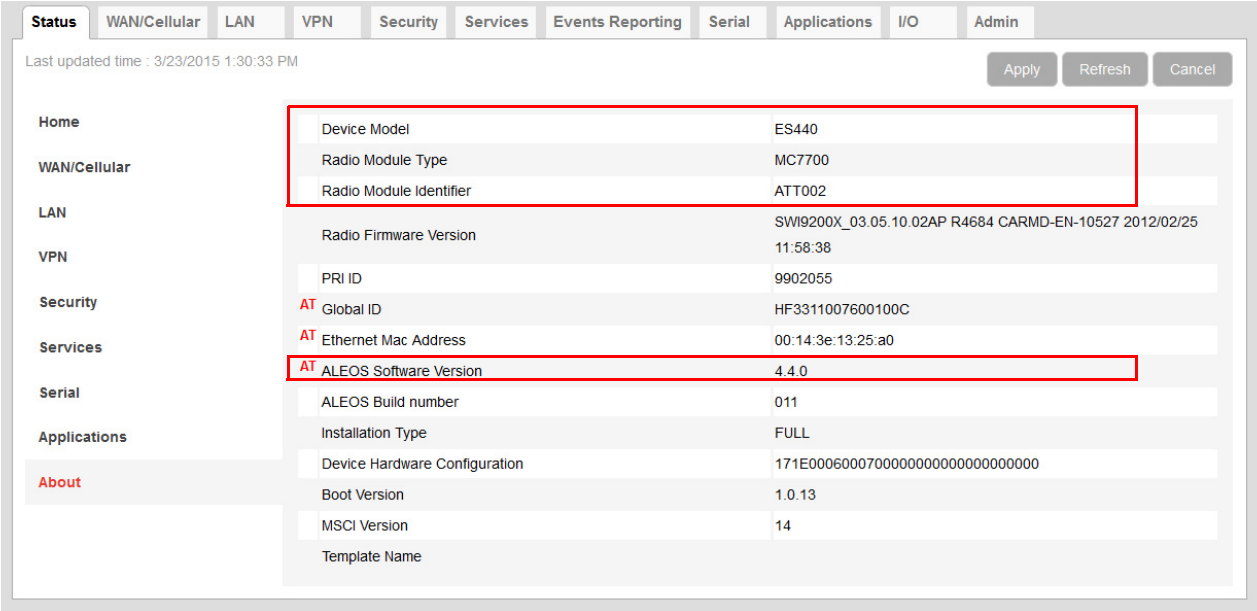


Figure 2-12: ACEmanager: Status > About

3. If you are planning to use ACEmanager to do the update:
   a. Go to source.sierrawireless.com and select your product and mobile network operator to get to the download page for your gateway.
   b. Download the new ALEOS software version for your system. If new radio module firmware is available, it is included with the ALEOS software in a .zip file. Do not install radio module firmware unless you are prompted to do so.

Note: If time of day reset (page 227) is enabled, Sierra Wireless recommends that you disable this feature before beginning the update.

Recommendations

If you have any questions about the update process, contact your authorized Sierra Wireless distributor before updating the radio module firmware.

Scheduling the update

The update can take up to 30 minutes to complete, depending on the speed of your network connection. The AirLink gateway being updated will be off-line during the update, so take this into account when scheduling the update.

Important: *BE PATIENT! The firmware update can take up to 30 minutes to complete. Ignore connection time out messages—the update process is still running.*

Waiting for the process to complete is faster than troubleshooting the problems that can be caused by interrupting the process midway. (Interrupting the process may result in having to return the gateway to the factory for repairs.)

Step 2—Update the ALEOS Software and Radio Module Firmware

Using ACEmanager to Update a Single AirLink gateway

To update the ALEOS software and radio module firmware on one AirLink gateway:

1. Connect the AirLink gateway you want to update to your laptop, launch your browser and enter the URL for the gateway. The default IP address/port for the Ethernet interface is http://192.168.13.31:9191. If it is a remote gateway, enter the domain name or public IP (WAN) address.

   Note: If you are connected to the gateway remotely, any files transferred to the gateway are transferred over-the-air and you may incur data charges.

2. Log in to ACEmanager.

   User name: user

   Default password: 12345

3. Go to Status > About and confirm that the current ALEOS version is 4.3.6. If not, see the note on page 18.

4. Click the Software and Firmware link.

   The Software and Firmware update window opens.

   Note: These instructions show typical Software and Firmware update windows. Details such as the ALEOS version, device model, radio firmware version, etc. may vary, depending on the gateway you are updating.

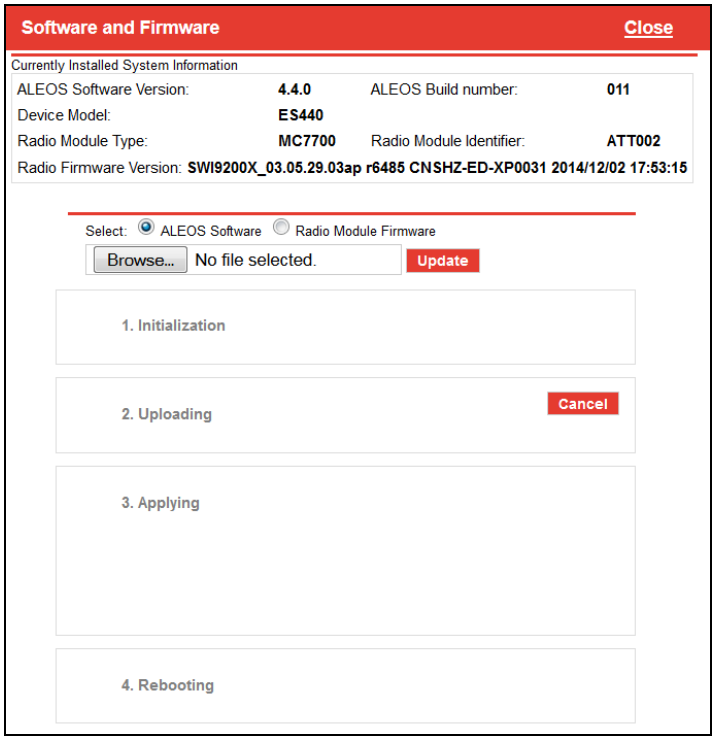


Figure 2-13: Software and Firmware update window

The update window gives you the option to update both ALEOS and the radio module firmware, or update only the radio module firmware. Unless advised otherwise by Sierra Wireless, we recommend that you select ALEOS software (which updates ALEOS and prompts you to update the radio module firmware if a newer version is available for your gateway).

5. Click Browse... and navigate to the ALEOS software you downloaded from the Sierra Wireless Web site.

Note: If you are updating only the radio module firmware, see Updating Only the Radio Module Firmware on page 25.

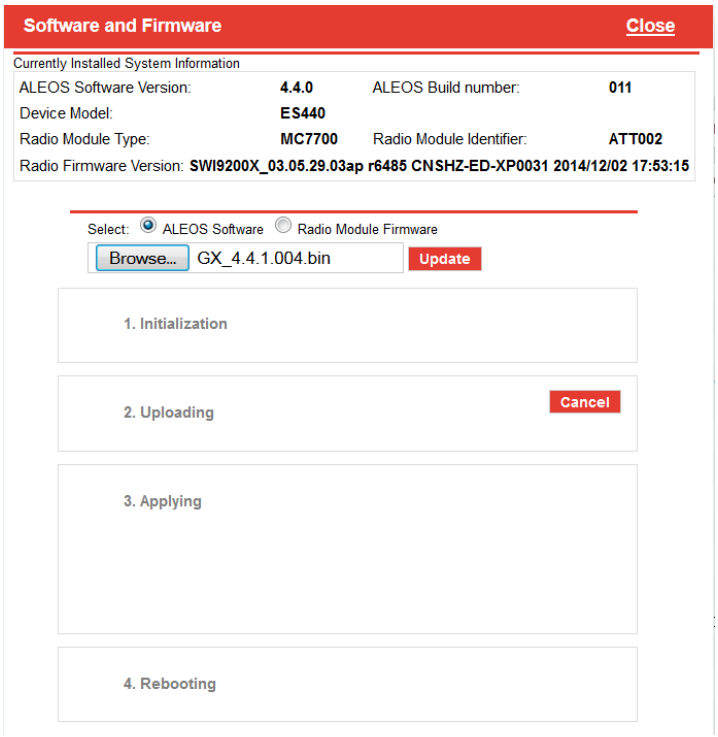


Figure 2-14: ALEOS file selected in Software and Firmware update window

6. Click Update.

   The ALEOS software update runs automatically and green check marks appear beside each step as it is completed.

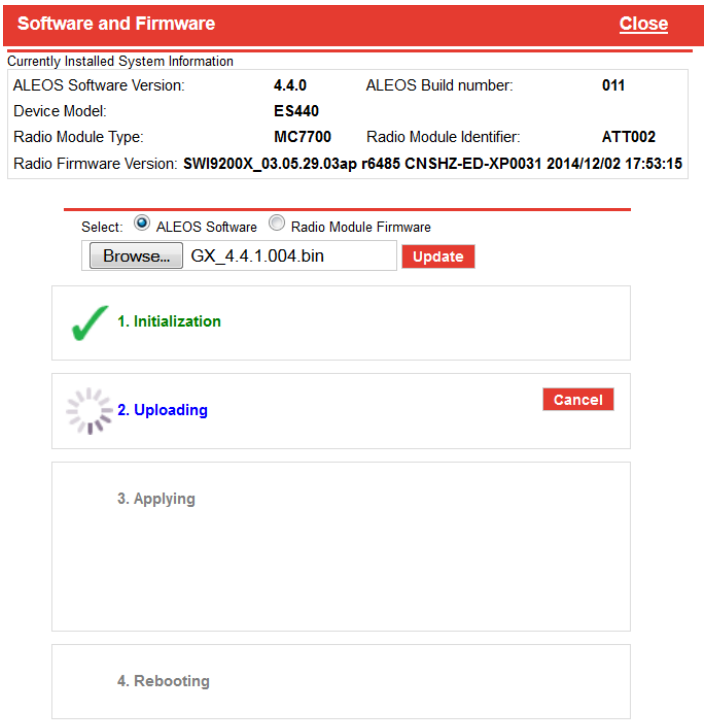


Figure 2-15: ALEOS software update in progress

Important: *Do not disconnect the AirLink gateway from the computer, and do not power cycle or reset the gateway during the update. If you see any error messages, refer to the* *Updating the ALEOS Software and Radio Module Firmware on page 335.*

7. Depending on the gateway and your Mobile Network Operator, you may be prompted to update the radio module firmware.

   If you do not receive a prompt, the radio firmware is up to date. Proceed to step 11.

   If you are prompted to update the firmware, proceed to step 8.

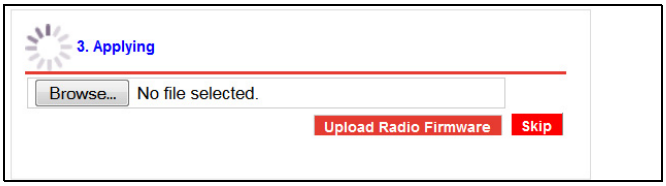


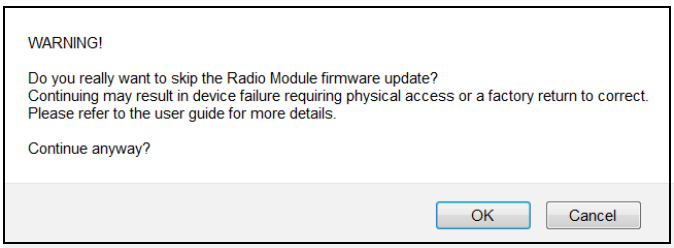
Figure 2-16: Prompt for Radio Module Firmware

8. Under Applying, click Browse... and navigate to the radio module firmware file that was included in the .zip file you downloaded.
9. Click Open.

   The firmware file name appears beside the Browse button.
10. Click Upload Radio Firmware.

    A message appears on the window indicating that the firmware has been successfully uploaded.

Note: Sierra Wireless recommends that you do NOT skip the radio module firmware update unless advised to do so by Sierra Wireless or an authorized distributor. If you choose to skip the radio module firmware update, you'll see the following warning.



Once the radio module firmware is uploaded, it begins applying the firmware upgrade. On the AirLink gateway, the LED chase begins to indicate that the firmware is being applied.

As indicated on the window, the radio module firmware may take 10 to 20 minutes to upload and install.

Important: *Do not disconnect the AirLink gateway from the computer or reboot the gateway while the firmware update is in progress. During the radio module firmware update, the gateway LEDs flash rapidly in sequence (an LED chase or caterpillar). When the radio module firmware update is complete, the gateway reboots automatically.*

If you see a message saying that the connection has timed out, ignore the message and continue to wait for the gateway to reboot.

If you clicked OK when you saw the timed out message and logged back in, you'll see the old version of the firmware. The firmware update process is still going on, so DO NOT reset the gateway or disconnect the power. DO NOT click Cancel. Continue to wait the 10 to 20 minutes for the radio module firmware update to complete. The gateway reboots once the firmware update is complete.

11. When the update is complete, the AirLink gateway reboots and you are returned to the Login screen.
12. When you see the Login screen, wait a few moments to ensure that the reboot is complete (or if you can see the gateway, check the LEDs) and then log in.
13. Go to Status > About.
14. Click Refresh.
15. Check the ALEOS Software Version and the Radio Firmware Version fields to confirm that the ALEOS software and the radio module firmware have been updated.

Using AirVantage Management Service (AVMS) to Update One or Multiple AirLink gateways Over-the-Air

You can use AirVantage Management Service to update the ALEOS software and radio module firmware over-the-air on one or multiple AirLink gateways.

If you don't have an AVMS account:

1. In ACEmanager, go to the Services tab and ensure that AVMS is enabled and the server URL is http://na.m2mop.net/msci/com. If this is not the case, enter the correct URL, click Apply and then click Reboot.

2. Go to www.sierrawireless.com/ALMS for more information.

Updating to ALEOS software with an AVMS account:

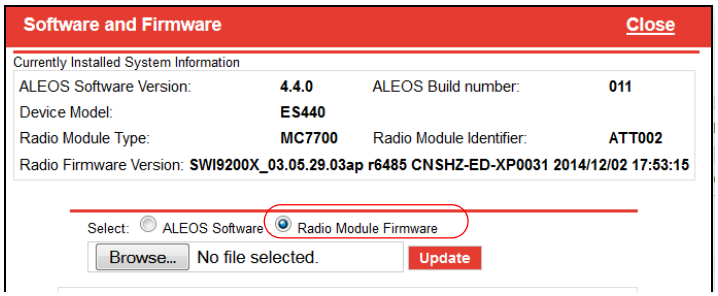
1. Go to airvantage.net and log in.
2. Follow the instructions in the online AVMS documentation to update the ALEOS software and radio module firmware.

Updating Only the Radio Module Firmware

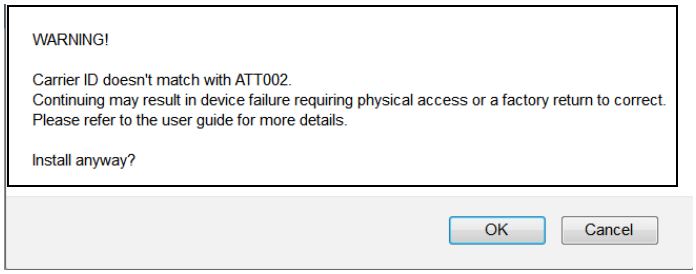
Note: Sierra Wireless recommends that you do NOT update only the radio module firmware unless advised to do so by Sierra Wireless or an authorized distributor.

If you are updating only the Radio Module Firmware:

1. Select the Radio Module Firmware button



2. Select the appropriate firmware file for your gateway and click Update. If you select a file for radio module firmware that is not supported on your gateway, you will see a warning message similar to the following:



   Unless you have been advised by Sierra Wireless to do so, we recommend that you do not install an unsupported version of the radio module firmware.

3. Click Update.

   The radio module firmware update runs automatically and green check marks appear beside each step as it is completed.

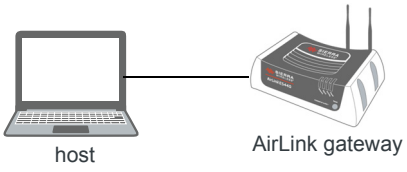
4. When the update is complete, the AirLink gateway reboots and you are returned to the Login screen.
5. When you see the Login screen, wait a few moments to ensure that the reboot is complete (or if you can see the gateway, check the LEDs) and then log in.
6. Go to Status > About.
7. Check the Radio Firmware Version has been updated.

Enterprise LAN Management

You can use AirLink gateways in the following configurations:

- Standalone with a connection to a single host

  When using the AirLink gateway with a single host, ensure that the host is DHCP enabled.

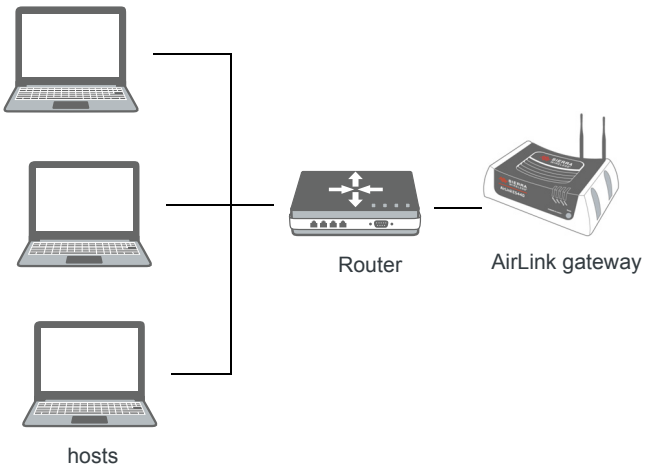


- With a router

  The router allows several hosts to use the AirLink gateway's connection to the network. When using the AirLink gateway with a router:
  - Configure the router to be DHCP enabled.

  And either:
  - Configure the router to use Network Address Translation (NAT).

    Or
  - Configure ALEOS (in ACEmanager) to use Host Port Routing. For information on using ALEOS with a router that is not configured to use NAT, see Host Port Routing on page 94.



Note: Other than for VLANs, ALEOS does not provide DHCP addresses to router connected hosts.

Over the Air (OTA) Connections

Access AirLink gateways

You can use an OTA connection to access AirLink gateways that are in either configuration described above (stand alone or with a router).

Access connected hosts

To use an OTA connection to access a connected host through the AirLink gateway, configure the host in ALEOS as the DMZ or port forwarding destination. For information on inbound OTA connections to the host, see DMZ on page 131 and Port Forwarding on page 126.

Configuring Your Gateway for use in a PCI Compliant System

The credit card industry requires retailers to comply with Payment Card Industry (PCI) standard to maintain a secure environment when processing payment card transactions. For these transactions, the AirLink ES Series gateway acts as a wireless data conduit for routers and PoSs (point-of-sale-terminals) that have been configured for PCI compliance.

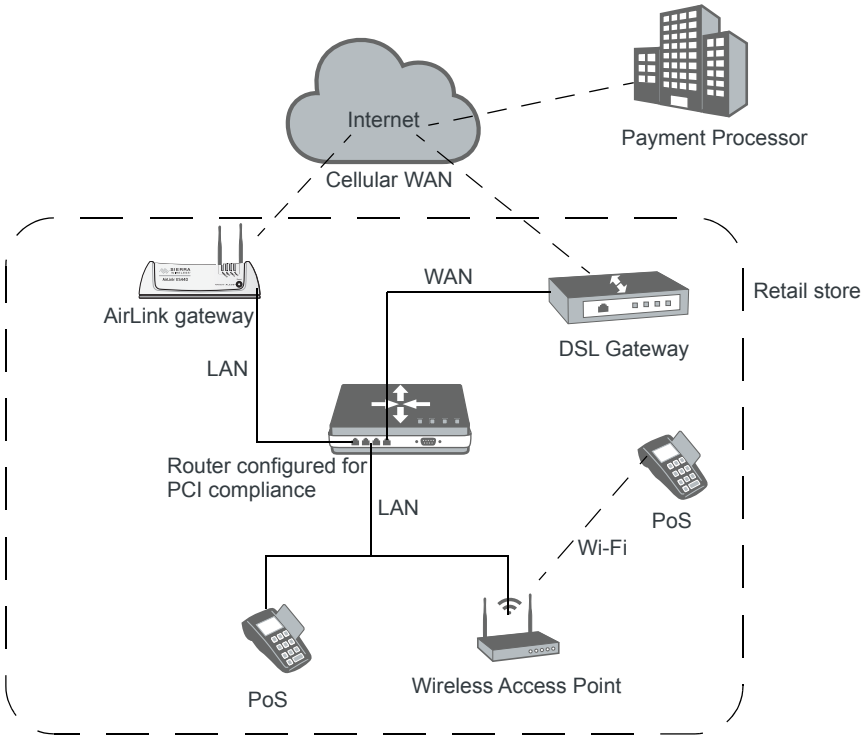


Figure 2-17: Sample PCI compliant network

The PCI compliant network must be set up so that:

- The USBnet is on a different subnet from the point-of-sale-terminal.
- All security protocols must be established from the point-of-sale terminal to the payment processor.
- Payment card terminals must be on a dedicated LAN or VLAN.
- The AirLink gateway must be connected to a router that is configured for PCI compliance.

Note: The serial port on the AirLink gateway has no access to the IP data path and does not need to be disabled.

If you are using the AirLink gateway for a payment card industry application, to meet PCI Data Security Standard compliance requirements the following steps must be done by a PCI certified service company.

For each gateway:

1. Connect the AirLink gateway to a router that has been configured for PCI compliance.
2. Log in to ACEmanager:
   - User Name: “user” (entered by default)
   - Default Password: 12345

   Note: For system security, and in accordance with PCI recommendations, ensure that you change the default ACEmanager password. The new password must be at least 8 characters long. For more information, see Change Password on page 224.
3. Go to Applications > ALEOS Application Framework and set the ALEOS Application Framework field to Disable.

3: Status

All of the fields in the Status group are read-only and provide information about the AirLink gateway. Depending on the individual settings and the onboard radio module, the actual status pages may look different than the screen shot shown here.

Tip: *To be sure you are viewing the current status for all fields, it's a good idea to first click the Refresh button on the upper right side of the screen.*

Home

The Home section of the Status tab is the first page displayed when you login to ACEmanager. It shows basic information about the WAN network connection, the mobile network connection, and important information about the gateway.

Note: The fields displayed vary depending on the gateway, the radio module, the type of network the gateway is connected to, and ACEmanager settings. For details, see Table 3-1 on page 34.

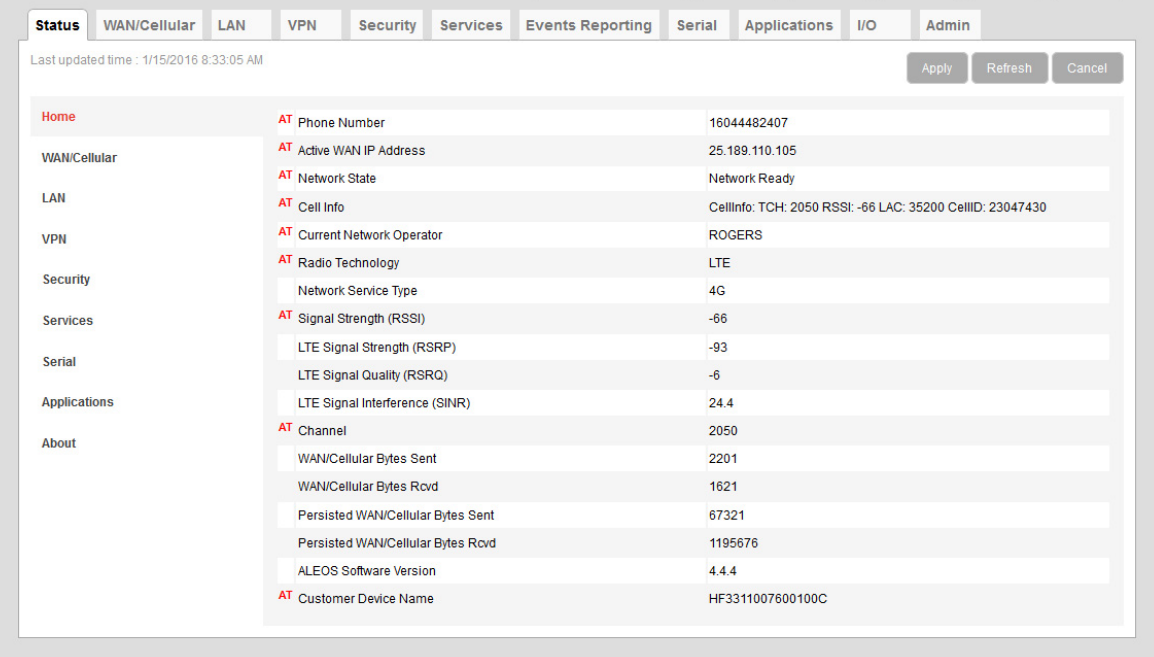


Figure 3-1: ACEmanager: Status > Home

Field	Description
Phone Number	The phone number associated with the Mobile Network Operator account. If the Mobile Network Operator does not allow the account to display the phone number or there is no Mobile Network account for the gateway, “NA” is displayed.
WAN Network	
Active WAN IP Address	The current IPv4 WAN IP address for the gateway.

Field	Description
Network State	Current state of the WAN network connection • Network Ready—Connected to a mobile broadband network and ready to transfer data • Network Ready Ethernet—Connected to an Ethernet network with a DHCP server. Note: This connection type has limited feature support. • Connecting To Network—Establishing a network connection; wait until the connection is established • Not Connected-Wait for Activity—The Always on connection field on the WAN/ tab (Advanced section) is set to Disabled. The gateway connects to the mobile network only when it needs to send or receive data. • Data connection failed. Waiting to retry—ALEOS is attempting to reconnect to the mobile broadband network. Ensure that the APN is correct or the account is activated to the ESN for your gateway. Wait until it is able to connect. If you see this status repeatedly or for an extended period of time, contact your Mobile Network Operator. • Network Link Down—Unable to connect to the network. Ensure that the APN is correct or the account is activated to the ESN for your gateway. If the problem persists, contact your Mobile Network Operator. • No SIM or Unexpected SIM Status—Unable to read the SIM information; check that the SIM card is installed correctly. • SIM PIN incorrect x attempts left—Wrong SIM PIN entered; enter the correct PIN. If the correct PIN is not entered in the specified number of attempts, the SIM is blocked. Contact your Mobile Network Operator to unblock the SIM. • No Service—Unable to connect to the broadband network. Check that the antenna is connected properly. If the problem persists, contact your Mobile Network Operator for information about coverage in your region. • Provisioning...—(CDMA networks only) The Mobile Network Operator is updating the radio module firmware with your account details. Wait until the provisioning is complete. • Awaiting provisioning...—(CDMA networks only) The gateway does not yet have an account associated with the radio module and is attempting to contact the Mobile Network Operator to obtain account information. If this state persists, check that the account is activated to the gateway's ESN. • Starting OMADM state—The Mobile Network Operator is starting an over-the-air (OTA) radio module gateway management session. Wait until the OTA management session is complete. • In NI PRL Update—(CDMA networks only) An updated Preferred Roaming List is being downloaded from the network. Wait until the download is complete. • NI PRL Failed—(CDMA networks only) The network initiated attempt to update the Preferred Roaming List failed. If the problem persists, contact your Mobile Network Operator. • NI PRL Failed. Waiting to retry—(CDMA networks only) The network initiated attempt to update the Preferred Roaming List failed. The network is waiting to retry the download. Wait until the download is complete. • Network Authentication Failed—Unable to connect to the network because of invalid authentication data. If the problem persists, contact your Mobile Network Operator. *Note: Messages displayed depend on the gateway, and the type of network.*
Mobile (Cellular) Network	
Cell Info	Cell information such as the Base Station Identity Code (BSIC), TCH, Received Signal Strength Indicator (RSSI), Location Area Code (LAC), and the cell ID For additional information, including cell info for LTE networks, see*CELLINFO2? on page 285 and LTE Networks on page 339.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Current Network Operator</td><td>Name of the Mobile Network Operator whose network the AirLink gateway is connected to

Note: The roaming operator is only displayed if the home operator allows this.</td></tr>
<tr><td>Radio Technology</td><td>Type of service being used by the gateway (e.g. LTE, HSPA+,1xRTT, EV-DO, UMTS, HSPA, EDGE or GPRS)
If you are connected to a network other than that of your Mobile Network Operator, the network service type indicates that you are roaming (and additional charges may apply).</td></tr>
<tr><td>Network Service Type</td><td>Type of network the gateway is connected to (e.g. 4G, 3G, 2G)</td></tr>
<tr><td colspan="2">Signal Strength and Quality
Different radio technologies have different ways of reporting signal strength and signal quality. The fields displayed in ACEmanager depend on the gateway product, the radio module, and the type of network it is connected to. Not all the fields described below appear on all gateways. For details, see Reported Signal Strength and Quality Values on page 34.</td></tr>
<tr><td>Signal Strength (RSSI)</td><td>Received Signal Strength Indicator
The average received signal power measured in the air interface channel
Indicates if there is a strong signal available for the AirLink gateway to connect to
See also LTE Signal Strength (RSRP) and LTE Signal Quality (RSRQ).
The value varies, depending on the network characteristics and the AirLink gateway.

<table>
<tr><th>RSSI</th><th>Signal strength</th></tr>
<tr><td>> -70 dBm</td><td>Excellent</td></tr>
<tr><td>-70 dBm to -85 dBm</td><td>Good</td></tr>
<tr><td>-86 dBm to -100 dBm</td><td>Fair</td></tr>
<tr><td>< -100 dBm</td><td>Poor</td></tr>
<tr><td>-110 dBm</td><td>No signal</td></tr>
</table>
</td></tr>
<tr><td>Signal Quality (ECIO)</td><td>2G/3G signal quality
Indicates the signal quality with a ratio of the average signal energy to co-channel interference in dB

<table>
<tr><th>EC/IO</th><th>Signal quality</th></tr>
<tr><td>0 to -6</td><td>Excellent</td></tr>
<tr><td>-7 to -10</td><td>Good</td></tr>
<tr><td>-11 to -20</td><td>Fair to Poor</td></tr>
</table>
</td></tr>
<tr><td>Received Signal Code Power (RSCP)</td><td>The RSCP is the power measured by the receiver on a particular physical channel. It provides an indication of signal strength for CDMA and UMTS connections. Expected values are in the range of -50 dB to -120 dB.</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>LTE Signal Strength (RSRP)</td><td>Reference Signal Received Power
The average signal power of all cell-specific reference signals within the LTE channel
Indicates whether the AirLink gateway has a strong connection to the wireless network
The value varies, depending on the network characteristics and the AirLink gateway.

<table><tr><th>RSRP</th><th>Signal strength</th></tr><tr><td>> -90 dBm</td><td>Excellent</td></tr><tr><td>-90 dBm to -105 dBm</td><td>Good</td></tr><tr><td>-106 dBm to -120 dBm</td><td>Fair</td></tr><tr><td>< -120 dBm</td><td>Poor</td></tr></table>
See also LTE Signal Quality (RSRQ) and Signal Strength (RSSI).</td></tr>
<tr><td>LTE Signal Quality (RSRQ)</td><td>Reference Signal Received Quality
The RSRQ indicates the quality of the AirLink gateway’s connection to the wireless network. (Is noise or interference affecting the quality of the connection?) See also Signal Strength (RSSI) and LTE Signal Strength (RSRP).
The value varies, depending on the network characteristics and the AirLink gateway.

<table><tr><th>RSRQ</th><th>Signal quality</th></tr><tr><td>> -9 dB</td><td>Excellent</td></tr><tr><td>-9 dB to -12 dB</td><td>Good</td></tr><tr><td>< -13 dB</td><td>Fair to Poor</td></tr></table>
Note: For additional information on the LTE network, use the *CELLINFO2? AT command (described on page 285).</td></tr>
<tr><td>LTE Signal Interference (SINR Level)</td><td>Signal Interference Plus Noise (SINR) Level only applies to Sprint and Verizon Wireless LTE networks. The maximum value for each level is:
• Level 0 = -9 dB
• Level 1 = -6 dB
• Level 2 = -4.5 dB
• Level 3 = -3 dB
• Level 4 = -2 dB
• Level 5 = +1 dB
• Level 6 = +3 dB
• Level 7 = +6 dB
• Level 8 = +9 dB</td></tr>
</table>

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>LTE Signal Interference (SINR)</td><td>Signal to noise and interference ratio
Higher values indicate that signal power is much greater than noise and interference.
<table><tr><th>SINR</th><th>Throughput</th></tr><tr><td>> 10</td><td>Excellent</td></tr><tr><td>6–10</td><td>Good</td></tr><tr><td>0–5</td><td>Fair</td></tr><tr><td>< 0</td><td>Poor</td></tr></table></td></tr>
<tr><td colspan="2">WAN Traffic</td></tr>
<tr><td>Channel</td><td>WAN network channel
The current active channel number for the mobile network connection</td></tr>
<tr><td>WAN/Cellular Bytes Sent</td><td>Number of bytes sent to the mobile network since system startup or reboot</td></tr>
<tr><td>WAN/Cellular Bytes Rcvd</td><td>Number of bytes received from the mobile network since system startup</td></tr>
<tr><td>Persisted WAN/ Cellular Bytes Sent</td><td>Number of bytes sent
The count starts when the gateway first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.</td></tr>
<tr><td>Persisted WAN/ Cellular Bytes Rcvd</td><td>Number of bytes received
The count starts when the gateway first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.</td></tr>
<tr><td colspan="2">Gateway Information</td></tr>
<tr><td>ALEOS Software Version</td><td>Version of ALEOS software currently installed on the gateway</td></tr>
<tr><td>Customer Device Name</td><td>By default, the name is the serial number of the gateway. If you have configured a device name in the IP Manager section of the Services > Dynamic DNS tab, that name appears in this field.</td></tr>
</table>

Table 3-1: Reported Signal Strength and Quality Values

Gateway	Radio Module[a]	Network	Signal Strength and Quality values
ES440	MC7750	CDMA	• Signal Strength (RSSI) • Signal Quality (ECIO) • Received Signal Code Power (RSCP)
	MC7700 MC7710	LTE/HSPA	• Signal Strength (RSSI) • Signal Quality (ECIO) • Received Signal Code Power (RSCP)

a. To determine the radio module for your gateway, in ACEmanager, go to Status > About.

WAN/Cellular

WAN/Cellular provides specific information about the connection including IP address and how much data has been transmitted or received. Some of the information on this screen is repeated on the Home page for quick reference.

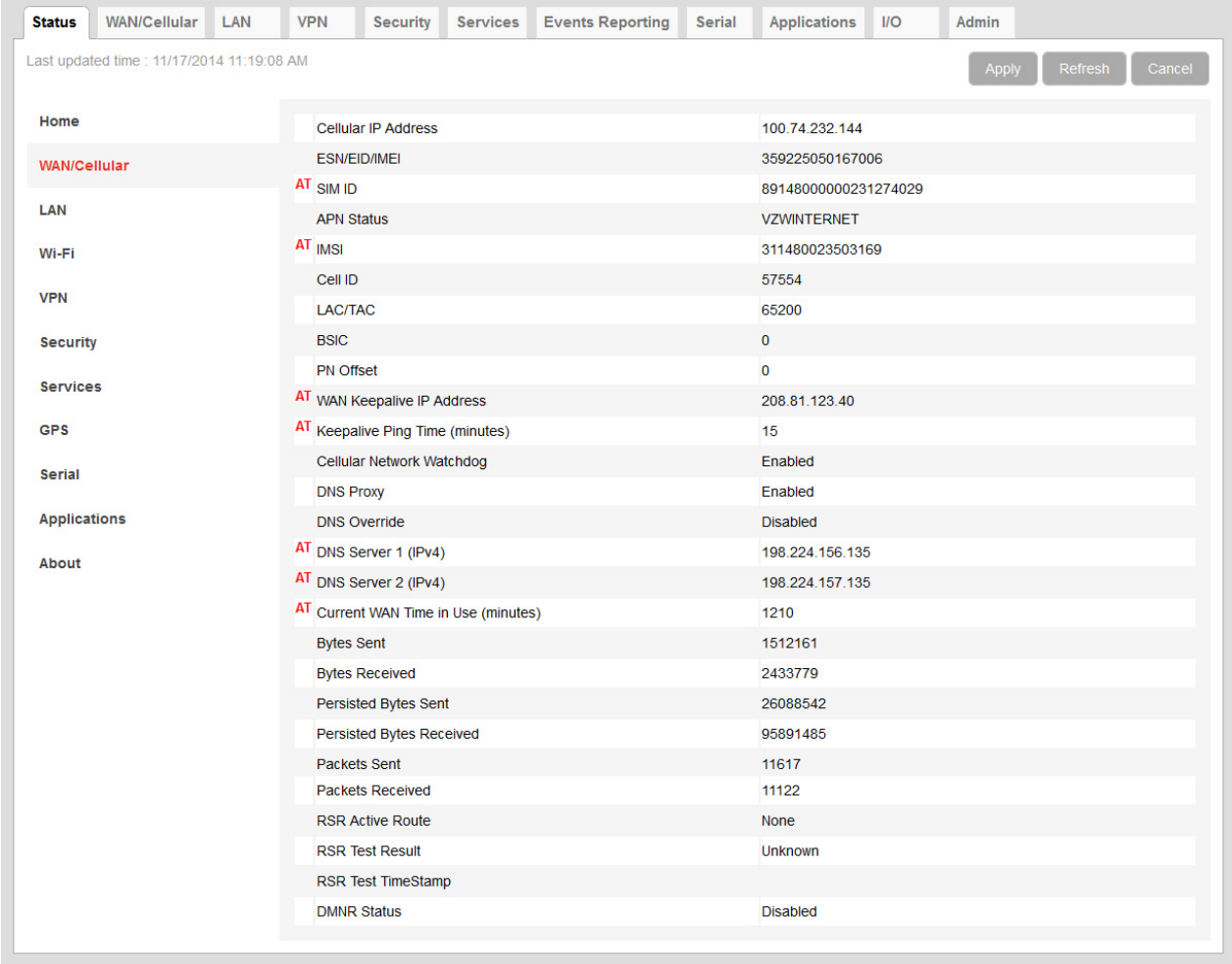


Figure 3-2: ACEmanager: WAN/Cellular — Sample screen

Field	Description
Cellular IP Address	IPv4 Cellular WAN IP Address If there is no mobile network connection, 0.0.0.0 is displayed.
IPv6 Address	This field is Verizon Wireless GX440-specific and only appears if the IP Address Preference field on the WAN/Cellular tab is set to IPv4 and IPv6 Gateway. If you have an IPv6 connection, this field displays the IP address. If not, it displays "::" (two colons).

Field	Description
IPv6 Prefix Length	This field is Verizon Wireless GX440-specific and only appears if the IP Address Preference field on the WAN/Cellular tab is set to IPv4 and IPv6 Gateway. Displays the length (number of bits) of the IPv6 Address Network Prefix.
WAN/Cellular Network Information The fields in ACEmanager depend on the gateway product, the radio module, and the type of network it is connected to. Not all the fields described below appear on all gateways.	
ESN/EID/IMEI	Electronic Serial Number for the internal radio
PRL Version	Version of the Preferred Roaming List installed in the gateway
PRL Update Status	Status of the last PRL (Preferred Roaming List) update. 0 if there has been none
SID	System ID
NID	Network ID
Band Class	CDMA band class
PN Offset	Base station identifier used in CDMA networks
SIM ID	Identification number for the SIM card in use
APN Status	Current APN in use by the network connection • (Auto Configured) is a default APN based on the SIM card in use. • (User Entered) is a custom APN entered manually into the configuration. *Note: APN is configured on the WAN/Cellular configuration tab.*
IMSI	International Mobile Subscriber Identity number
Cell ID	Unique number that identifies each base transceiver station (BTS) or sector of a BTS within an LAC
LAC/TAC	Location Area Code or Tracking Area Code (LTE)
BSIC	Base Station Identity Code
WAN Keepalive IP Address	IP address that WAN Keep Alive uses to test the WAN network connectivity (see WAN Keepalive IP Address on page 60.)
Keepalive Ping Time (minutes)	Amount of time between Keepalive pings in minutes
Cellular Network Watchdog	Status of the Cellular Network Watchdog (Enabled or Disabled) See Cellular Network Watchdog on page 55.
DNS Proxy	Determines which DNS server the connected clients use for domain name resolution • Enable—DNS Proxy is activated. Connected DHCP clients acquire the AirLink gateway's IP address as their DNS server. The AirLink gateway performs DNS lookups on behalf of the clients. • Disable—Connected DHCP clients acquire the DNS servers used by the gateway. To set this option, see DNS Proxy on page 97.

Field	Description
DNS Override	Override WAN-granted DNS • Enabled—Locally configured DNS servers are used. • Disabled—DNS servers provided by the active WAN connection are used.
DNS Server 1 (IPv4)	1st DNS server IP address currently in use by the WAN connection to resolve domain names into IP addresses
DNS Server 2 (IPv4)	2nd DNS server IP address
Current WAN Time in Use (minutes)	The time, in minutes, that the gateway has been connected to the current WAN network. *Note: The value of this field is 0 if the gateway is not connected to a WAN mobile network.*
Bytes Sent	Number of bytes sent to the mobile network since system startup or reboot
Bytes Received	Number of bytes received from the network since system startup or reboot
Persisted Bytes Sent	Number of bytes sent The count starts when the gateway first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.
Persisted Bytes Received	Number of bytes received The count starts when the gateway first goes on air and persists over reboot. The field resets to zero on reset to factory default settings.
Packets Sent	Number of packets sent to the network since system startup or reboot
Packets Received	Number of packets received from the network since system startup or reboot
RSR Active Route	Active route for Reliable Static Routing • Primary—Specified network traffic is currently using the configured primary route. • Backup—Specified network traffic is currently using the configured backup route. • None—RSR is not enabled.
RSR Test Result	Result of the most recent Object Tracking test
RSR Test TimeStamp	Time of the most recent Object Tracking test
Dynamic Mobile Network Routing (DMNR) is only supported on the Verizon Wireless network.	
DMNR Status	DMNR status: • Enabled • Disabled

Field	Description
DMNR Foreign Agent Registration Status	This field only appears if DMNR is enabled. The status of transactions with the Home agent • Pass—Connected subnets registered or de-registered successfully • Fail—Unable to register or de-register connected subnets • Unknown
DMNR Reverse Tunnelling Agent Status	This field only appears if DMNR is enabled. Status of the NEMO tunnel • Up • Down

LAN

Table 3-2: Reported WAN/Cellular Status Values

WAN/Cellular Status	Gateway and Radio Module[a]	
	ES440 (MC7750)	ES440 (Mc77x0), ES450
ESN/EID/IMEI	✓	✓
PRL Version	✓	
SID	✓	
NID	✓	
Band Class	✓	
PN Offset	✓	
SIM ID	✓	✓
APN Status	✓	✓
IMSI	✓	✓
Cell ID	✓	✓
LAC/TAC	✓	✓
BSIC	✓	✓

a. To determine the radio module for your gateway, in ACEmanager, go to Status > About.

This is the status of the local network. It lists information about the network and connected clients.

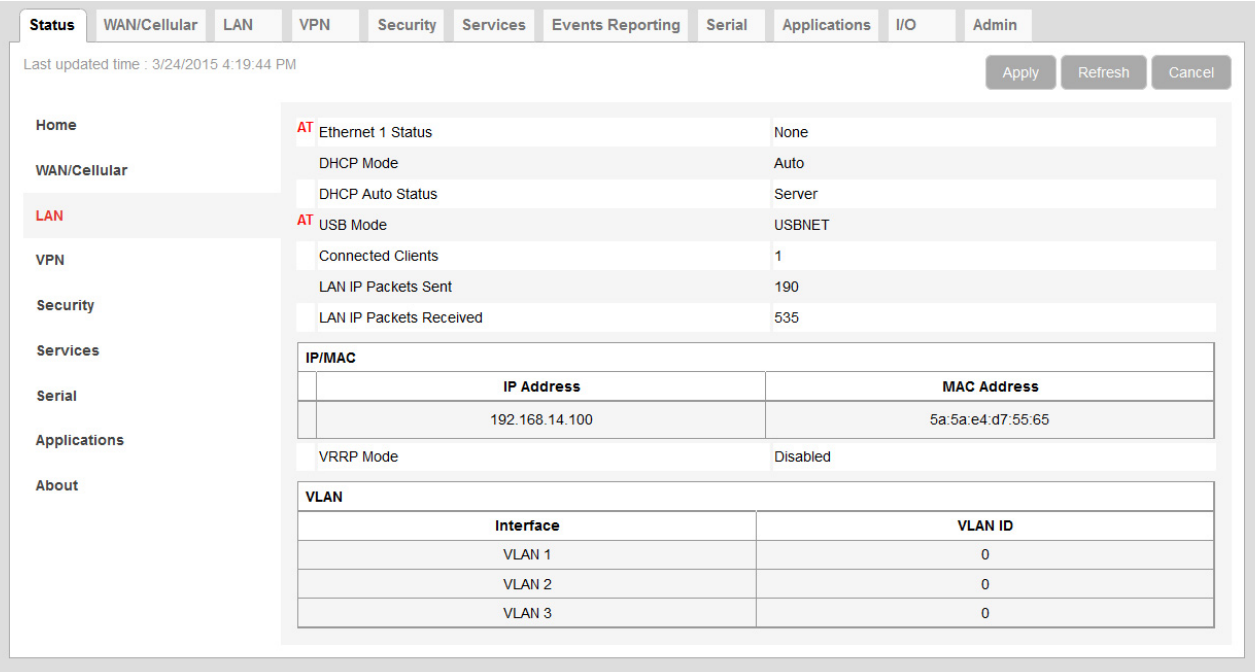


Figure 3-3: ACEmanager: Status > LAN

Field	Description
Ethernet 1 Status	Speed and duplex status of the connection on Ethernet port 1 (the main Ethernet port). If there is no connection, the value is None.
DHCP Mode	Status of DHCP mode • Server—The AirLink gateway is acting as a DHCP server for all Ethernet connections. • Disable—The AirLink gateway is acting as neither a DHCP server or client. All devices connected to the AirLink gateway must have a static LAN IP or use PPPoE. • Auto—Default setting is used by authorized AirLink resellers for initial gateway configuration. See DHCP Auto Status for more information.
DHCP Auto Status	Status of DHCP Auto mode (This field only appears when the DHCP mode is Auto.) • Server—ALEOS is acting as a DHCP server. • Client—ALEOS is acting as a DHCP client.
USB Mode	Which USB port mode is set (USBnet, USB serial, or Disabled)
Connected Clients	Number of connected devices that obtained their IP address through DHCP over Ethernet or USBnet. The value in this field does not include devices connected via PPP or PPPoE.
LAN IP Packets Sent	Number of IP packets sent to the Ethernet host interface since the system startup
LAN IP Packets Sent	Number of IP packets sent to the Ethernet host interface since the system startup
LAN IP Packets Received	Number of IP packets received from the Ethernet host interface since the system startup
LAN IP Packets Received	Number of IP packets received from the Ethernet host interface since the system startup

Field	Description
IP/MAC table	Local IP Address and the MAC Address of connected devices that obtain their IP address through DHCP. *Note: IPv6 clients are not shown.*
VRRP Enabled	Configuration of the VRRP feature
VLAN table	Identities (Interface name and ID) of the configured VLANs

VPN

The VPN section gives an overview of the VPN settings and indicates whether a VPN connection has been made.

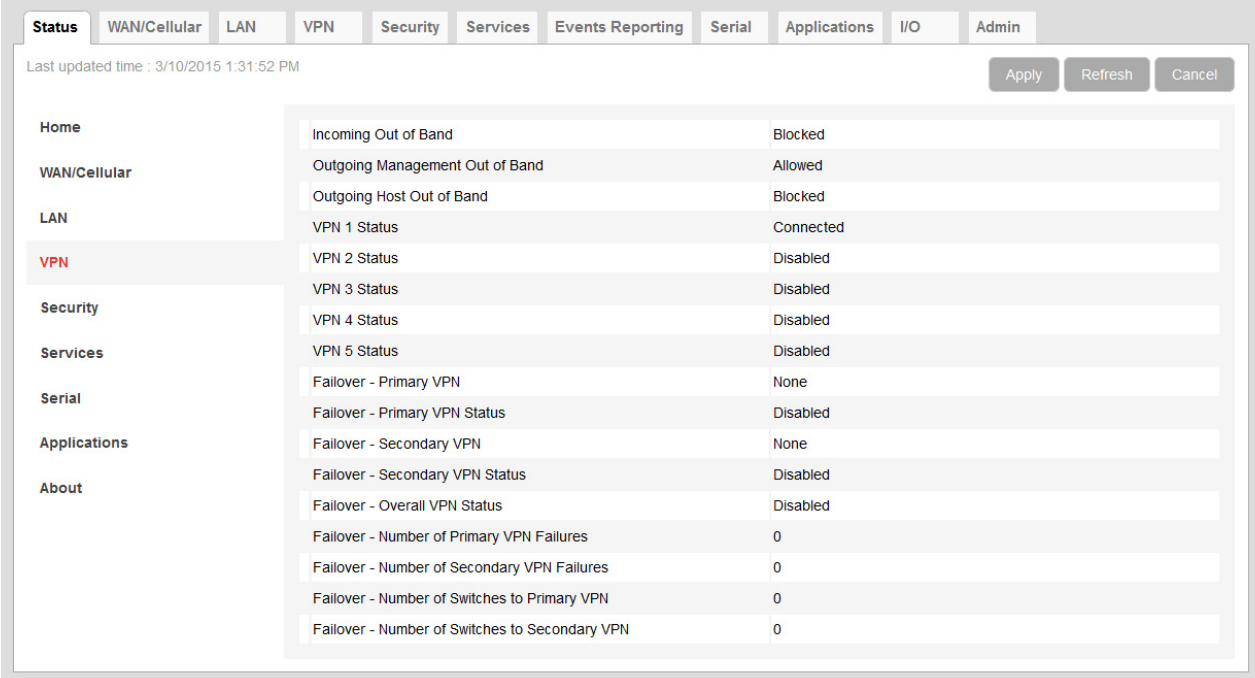


Figure 3-4: ACEmanager: Status > VPN

Field	Description
Incoming Out of Band	Whether Incoming Out of Band traffic is allowed or blocked
Outgoing Management Out of Band	Whether outgoing ALEOS Out of Band traffic is allowed or blocked
Outgoing Host Out of Band	Whether Outgoing Host Out of Band traffic is allowed or blocked

Field	Description

VPN 1 to 5 Status	Status of each VPN connection:
	• Disabled—VPN is disabled (default)
	• Not Connected—The VPN failed to connect. This could be because of a mismatch in the configuration between the client and the server, no data connection on the gateway, etc.
	• Connected—The VPN is connected and ready to transmit traffic.
	• Configuration Error—This status appears when:
	  • Two VPNs have both the same Local Address and the same Remote Address
	  • More than one VPN has the remote address set to “0.0.0.0”
	  Note: This restriction does not apply to the Additional Remote Subnets.
	When either of these errors exist, only the first of the conflicting VPNs is operational.
	To determine which VPNs are in conflict:
	1. Go to Admin > Configure Log.
	2. For the VPN Subsystem, ensure that Display in Log is set to Yes. The Verbosity can be either Info or Debug.
	3. Click View Log.
	4. The resulting log shows you which VPNs are in conflict.

Failover - Primary VPN	ID of the Primary VPN (for VPN Failover) i.e. VPN 1, VPN 2, VPN 3, VPN 4, VPN 5, or None (Default is None.) Setting persists over reboot.
Failover - Primary VPN Status	Status of the Primary VPN: • Disabled—VPN Failover is disabled. (default) • Connecting—The VPN is trying to connect to the responder. • Active—The VPN tunnel is ready and transferring traffic. • Backup—This is currently the backup VPN connection. • Failed—Dead Peer Detection (DPD) has determined that the VPN responder is dead, or a ping sent to the VPN host failed. • Out of Service—There have been 5 DPD failures within an hour.
Failover - Secondary VPN	ID of the Secondary VPN (for VPN Failover) i.e. VPN 1, VPN 2, VPN 3, VPN 4, VPN 5, or None (Default is None.) Setting persists over reboot.
Failover - Secondary VPN Status	Status of the Secondary VPN: • Disabled—VPN Failover is disabled. (default) • Connecting—The VPN is trying to connect to the responder. • Active—The VPN tunnel is ready and transferring traffic. • Backup—This is currently the backup VPN connection. • Failed—Dead Peer Detection (DPD) has determined that the VPN responder is dead, or a ping sent to the VPN host failed. • Out of Service—There have been 5 DPD failures within an hour.

Field	Description
Failover - Overall VPN Status	Status of the overall VPN: • Disabled—VPN Failover is disabled. (default) • Connecting—One of the VPNs is trying to connect to the responder. • Active—One VPN tunnel is currently in use. The backup VPN is available. • Backup_Unavailable—One VPN tunnel is currently in use. The backup VPN is not available. • Out of Service—Neither the primary nor secondary VPN is operational. • N/A—The overall VPN status is temporarily not available. Click Refresh.
Failover - Number of Primary VPN Failures	Number of times DPD has failed on the Primary VPN since the gateway has been rebooted or the “Set VPN Policy” button was clicked
Failover - Number of Secondary VPN Failures	Number of times DPD has failed on the Secondary VPN since the gateway has been rebooted or the “Set VPN Policy” button was clicked
Failover - Number of Switches to Primary VPN	Number of times traffic was switched to the Primary VPN since the gateway has been rebooted or the “Set VPN Policy” button was clicked
Failover - Number of Switches to Secondary VPN	Number of times traffic was switched to the Secondary VPN since the gateway has been rebooted or the “Set VPN Policy” button was clicked

Security

The security section provides an overview of the security settings on the AirLink gateway.

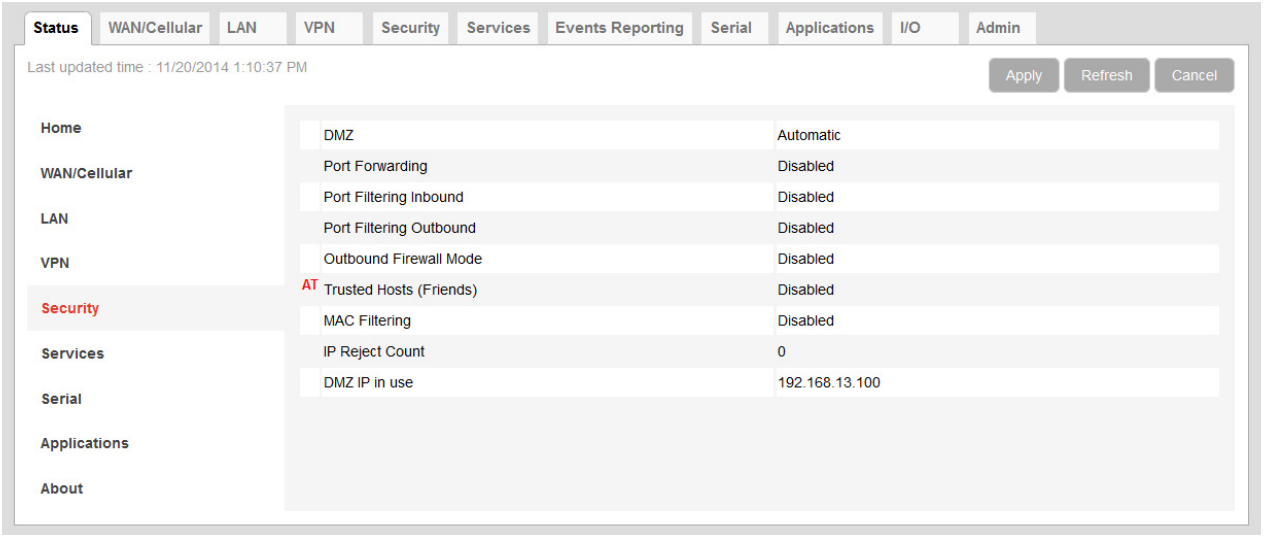


Figure 3-5: ACEmanager: Status > Security

Field	Description
DMZ	Status of DMZ (Automatic, Manual, or Disabled) DMZ defines a single LAN connected device where all unsolicited data should be routed.
Port Forwarding	Status of port forwarding (Enabled or Disabled)
Port Filtering Inbound	Status of inbound port filtering (Allowed Ports, Blocked Ports, or Disabled)
Port Filtering Outbound	Status of outbound port filtering (Allowed Ports, Blocked Ports, or Disabled)
Outbound Firewall Mode	Status of the outbound firewall (Enabled or Disabled)
Trusted Hosts (Friends)	Status of the Trusted Hosts (Friends) list (Disabled or Enabled) When this option is enabled, the AirLink gateway only accepts connections from trusted remote IP addresses.
MAC Filtering	Status of MAC filtering (Enabled or Disabled)
IP Reject Count	Number of IP addresses that have been rejected
DMZ IP in use	IP address currently in use for DMZ

Services

This section shows the status of AirLink services, including the ACEmanager access level.

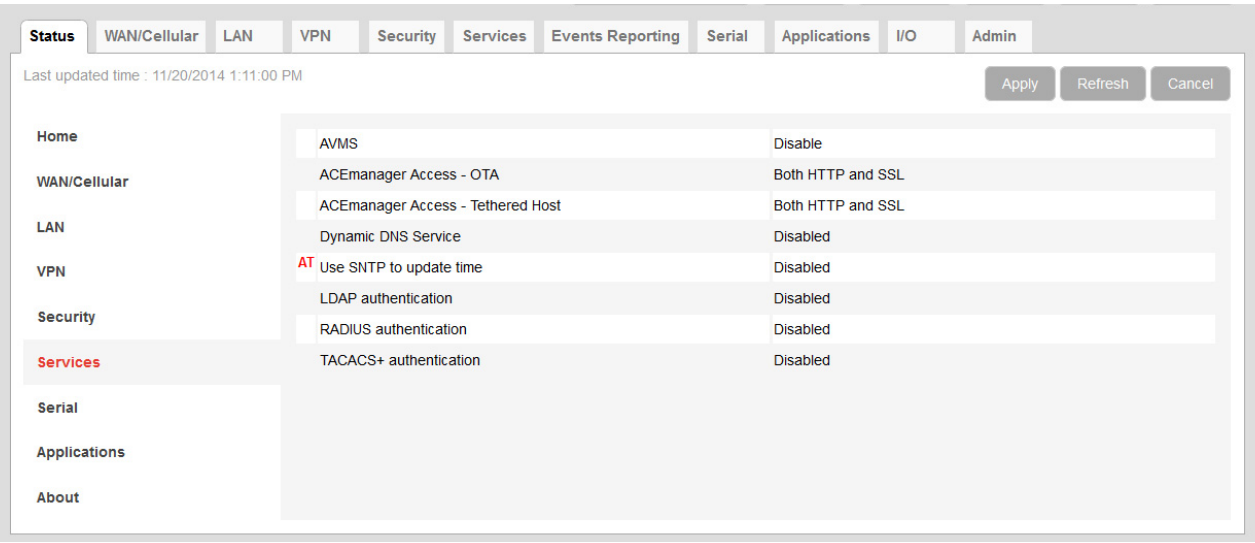


Figure 3-6: ACEmanager: Status > Services

Field	Description
AVMS	Status of the connection to the AirVantage Management Service
ACEmanager Access - OTA	ACEmanager over-the-air access mode (OFF, SSL Only, or Both HTTP and SSL [default])
ACEmanager Access - Tethered Host	ACEmanager access if tethered (physically connected) to Ethernet, USB, or RS232 (SSL Only or Both HTTP and SSL [default])
Dynamic DNS Service	Service in use for Dynamic DNS translation
Full Domain Name	If the Dynamic DNS Service is configured to use a 3rd party host, the domain name configured is displayed. If the Dynamic DNS Service is configured to use IP Manager, this field does not display.
Use SNTP to update time	Daily SNTP updates of the system time
LDAP Authentication	Status of the LDAP client: • Enabled • Disabled (default)
RADIUS Authentication	Status of the RADIUS client: • Enabled • Disabled (default)
TACACS+ Authentication	Status of the TACACS+ client: • Enabled • Disabled (default)

Serial

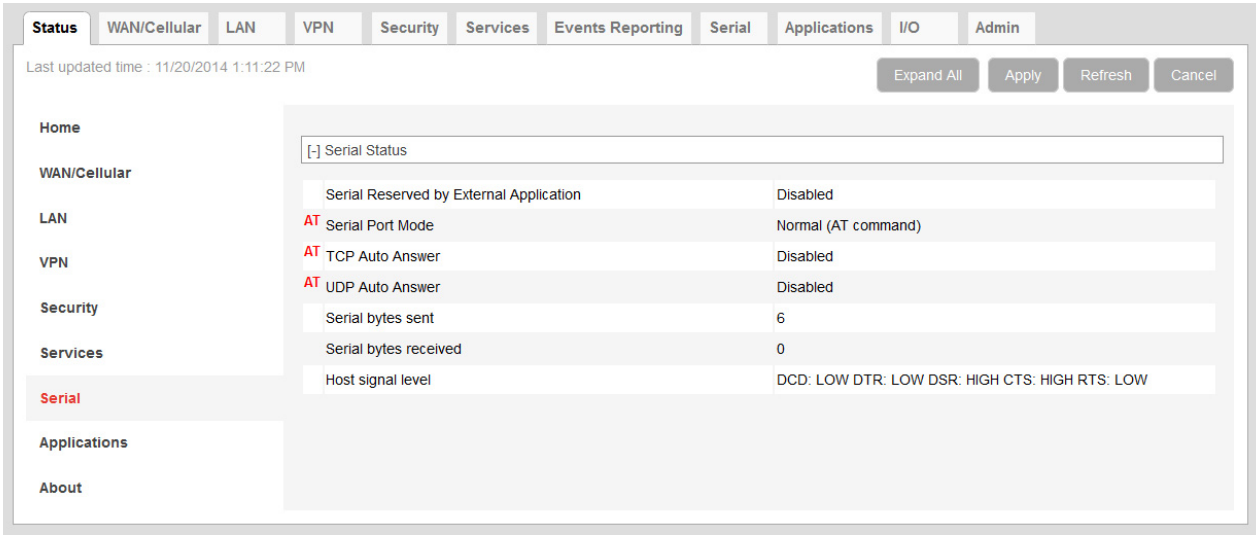


Figure 3-7: ACEmanager: Status > Serial

Field	Description
Serial Reserved by External	Reservation status of the serial port: • Enabled—The serial port is reserved for ALEOS Application Framework (AAF), and cannot be used for any other serial-related ALEOS features. • Disabled—The serial port is available for non-AAF, serial-related ALEOS features. To reserve the serial port for AAF, go to Applications > ALEOS Application Framework > Serial Port Reserved. (See ALEOS Application Framework on page 217.)
Serial Port Mode	Default power-up mode for the serial port. When the AirLink gateway is power-cycled, the serial port enters the mode specified by this command after 5 seconds.
Autologin reverse telnet	This field only appears when reverse telnet is selected as the Serial Port Mode. Status of autologin for reverse telnet. For more information, see Reverse Telnet/SSH on page 196.
TCP Auto Answer	This parameter determines how the AirLink gateway responds to an incoming TCP connection request. The AirLink gateway remains in AT Command mode until a connection request is received. DTR must be asserted (S211=1 or &D0) and the gateway must be set for a successful TCP connection. The AirLink gateway sends a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgment of the connection request and the TCP session is established. • Disabled (default) • Enabled
UDP Auto Answer	How UDP auto answer mode is configured • Disabled (default) • Enabled
Serial bytes sent	Number of bytes sent over serial port to host
Serial bytes received	Number of bytes received over serial port from host
Serial Signal Level	Status of the following parameters related to the host signal level: • DCD—Data Carrier Detect—Control signal to the PC • DTR—Data Terminal Ready—Used to establish a connection • DSR—Data Set Ready—Used to establish a connection • CTS—Clear to Send—Data flow control • RTS—Request to Send—Data flow control Each parameter can have a value of LOW (signal not asserted) or HIGH (signal being asserted). The first three parameters (DCD, DTR, and DSR) may be helpful for troubleshooting. If the values shown for these parameters are not as expected: 1. Press Refresh to ensure you have the latest values. 2. Check the cable connections. *Note: ACEmanager does not update dynamically. Press Refresh to view the current values.*

Applications

The Applications section of the Status group provides information on the status of data service.

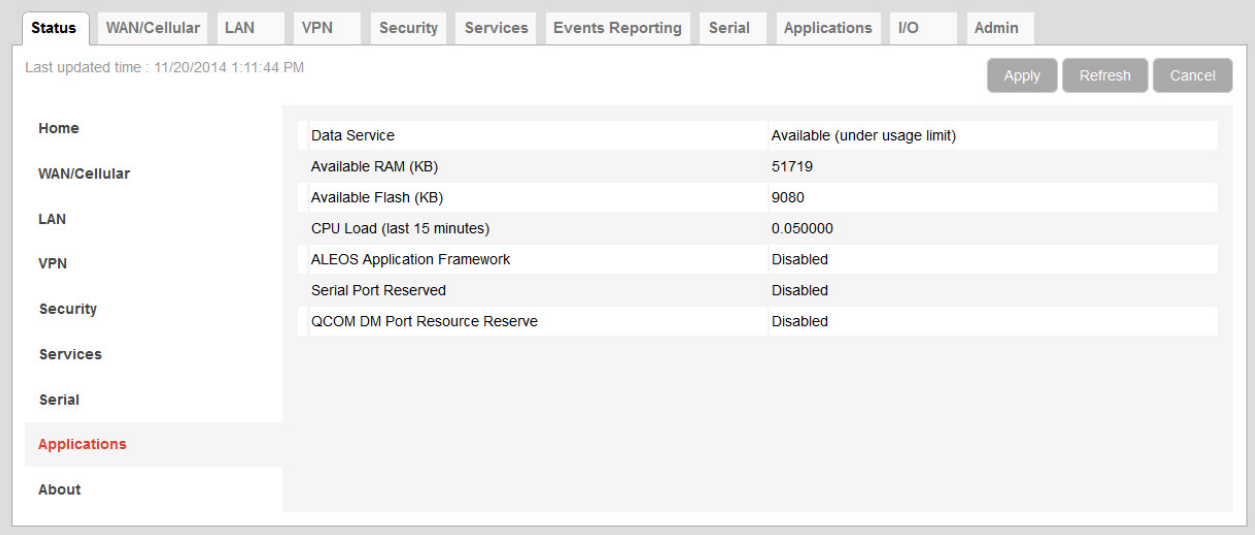


Figure 3-8: ACEmanager: Status > Applications

Field	Description
Data Service	Data Service field displays “Available (under usage limit)” if the configured usage limit has not been exceeded.
Available RAM (KB)	Available RAM in kilobytes (1000 bytes), updated every 30 seconds
Available Flash (KB)	Available Flash on the user partition in kilobytes (1024 bytes), updated every 30 seconds
CPU Load (Last 15 minutes)	CPU load, averaged over the last 15 minutes and updated every 30 seconds The CPU load relates to how many applications are attempting to execute in parallel over the 15-minute period. If the load is greater than 1, some applications are waiting for CPU capacity to become available and may be delayed in launching.
ALEOS Application Framework	Whether ALEOS Application Framework is enabled or disabled
Serial Port Reserved	Reservation of the serial port: • Disable (default) • Enable
QCOM DM Port Resource Reserve	Reservation of the QCOM DM port: • Disable (default) • Enable

About

The About section of the Status group provides basic information about the AirLink gateway. The fields for this section provide the same information for the CDMA, GSM, and LTE wireless standards.

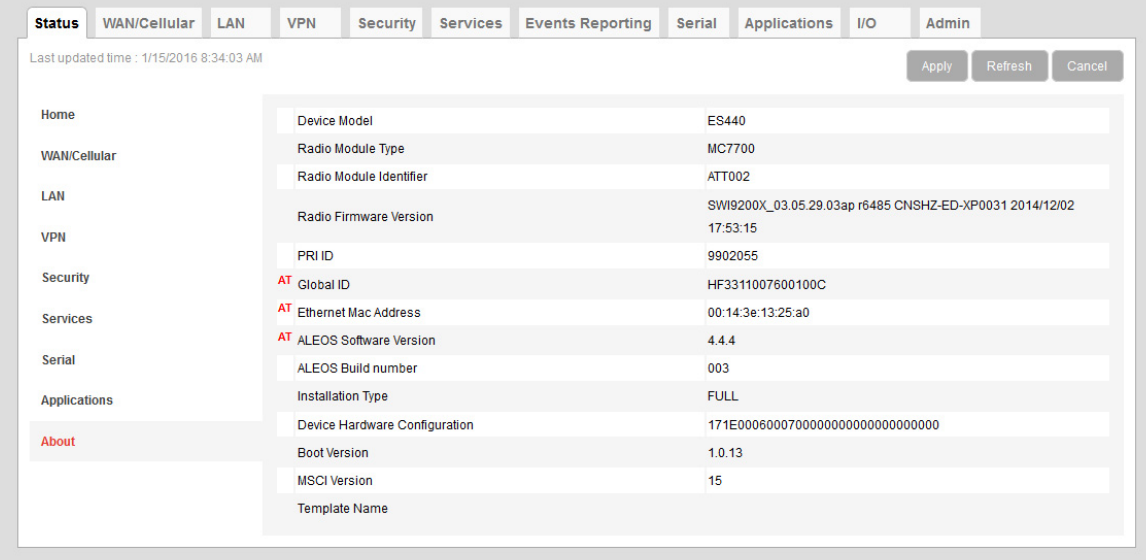


Figure 3-9: ACEmanager: Status > About

Field	Description
Device Model	Model of the gateway (e.g., ES440)
Radio Module Type	Model number of the internal radio module (e.g. MC7700)
Radio Module Identifier	Identifier for the internal mobile radio module
Radio Firmware Version	Firmware version in the radio module
PRI ID	Product Release Instructions ID number
Global ID	Device ID used by ALEOS to identify itself for various management applications
Ethernet Mac Address	MAC address of the main Ethernet port
ALEOS Software Version	Version of ALEOS software running on the AirLink gateway
ALEOS Build number	Build number for the ALEOS Software
Installation Type	Full or incremental
Device Hardware Configuration	AirLink gateway's hardware configuration
Boot Version	Version of boot code installed in the gateway
MSCI Version	MSCI version of the ALEOS internal configuration database

Field	Description
Template Name	If you have installed a custom-named template, the name appears here. Otherwise, the field is blank.
Module CDMA check	This field only appears on AirLink gateways with radio module MC7750. Shows the status of the module CDMA parameters. Possible values are: • Success—Module CDMA parameters are valid. • Fail—Module CDMA parameters are not valid. *Note: If the check fails, this field is empty. (Status is unknown.)*

4: WAN/Cellular Configuration

The WAN/Cellular tab in ACEmanager allows you to view and modify mobile network connection settings. The settings available depend on the gateway model and the radio module.

The first time you power up the gateway on its home network, it automatically begins the activation/provisioning process and attempts to connect to the network. This process typically takes 5–10 minutes. If the gateway does not automatically connect to the network, see Network Credentials on page 52.

Note: The fields displayed vary depending on the gateway, the radio module installed in the gateway, and ACEmanager settings.

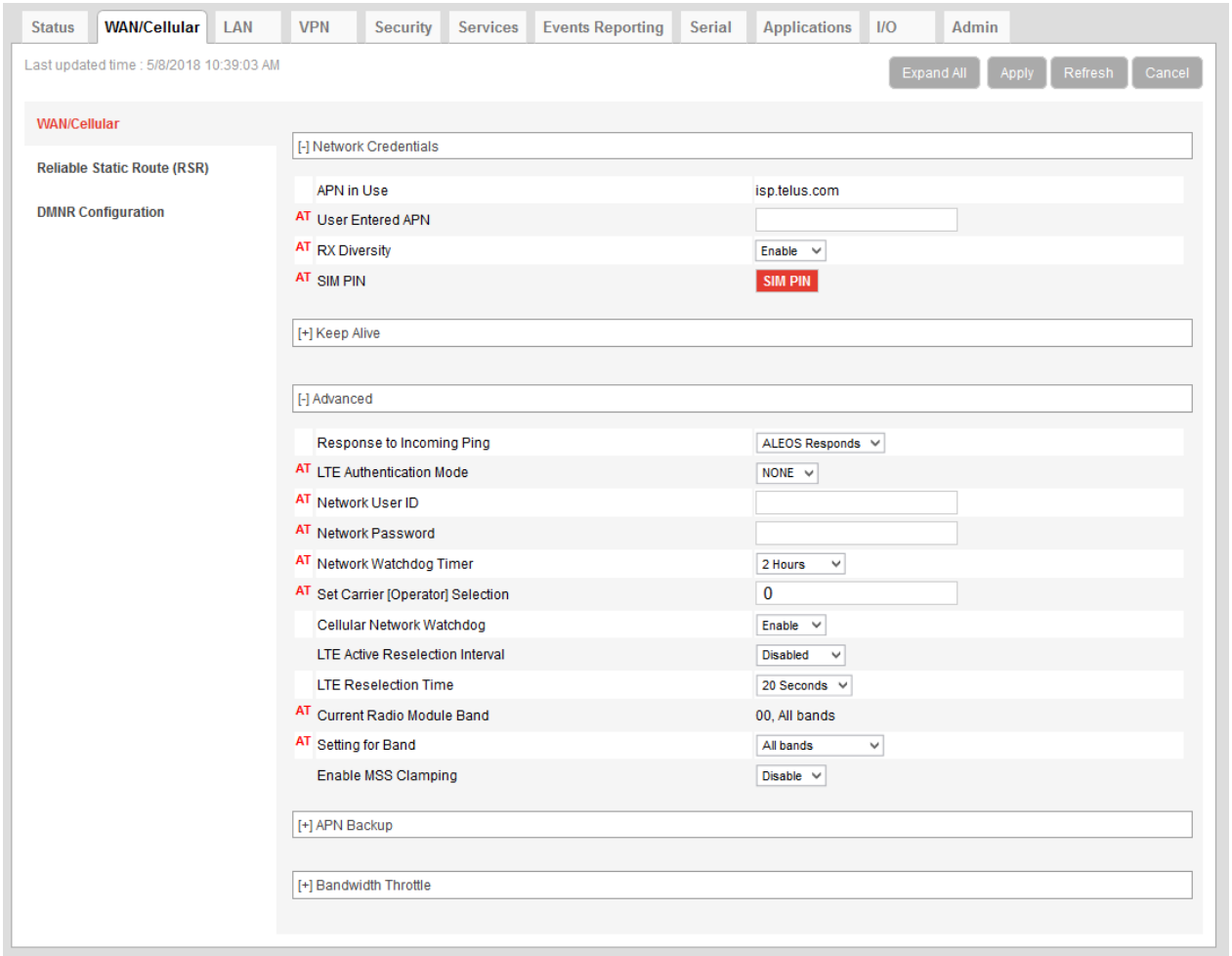


Figure 4-1: ACEmanager: WAN/Cellular — Sample screen

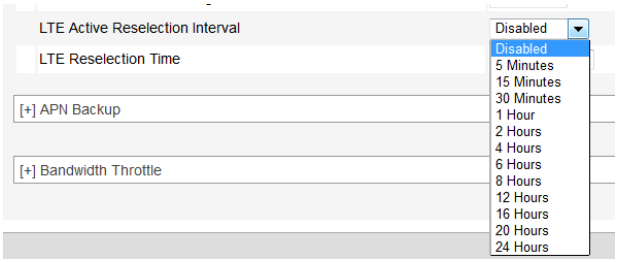
Field	Description
Network Credentials	
• *If the gateway does not automatically connect to the network, you may need to manually configure your APN using the User Entered APN field. You may also need to contact your Mobile Network Operator to confirm the APN and activation status of your gateway.*	
Note: Network credentials shown depend on the gateway, the radio module, and the network. Not all fields appear on all gateways. For details, see WAN/Cellular > Network Credentials on page 59.	
APN in Use	The APN in use for the current mobile network connection. When you power on the AirLink gateway, the APN the gateway is using for authentication on the mobile network is displayed. • If a User Entered APN is configured, the User Entered APN is displayed. • If there is no User Entered APN configured, an automatically-selected APN is displayed. • When the Backup APN is configured, the APN in Use displays the configured Backup APN when it is being used for authentication on the mobile network. If ALEOS is unable to find the appropriate APN to use (No APN found), contact your Mobile Network Operator for the APN and enter it in the User Entered APN field.
User Entered APN	The APN entered in this field takes priority over the automatically-selected APN. 1. Enter the APN in this field (maximum 100 characters). 2. Click Apply. 3. Click Reboot. *Note: If you reset the gateway to factory defaults, you have the option to preserve the custom APN, if entered. See Reset Mode on page 232.*
RX Diversity	Allows two antennas to provide a more consistent connection • Disable • Enable (default) If you are not using a diversity antenna, diversity should be disabled. *Note: This field is not available for all AirLink gateways.*
SIM PIN	Click this button to configure the PIN stored on the AirLink gateway. For more information, see SIM PIN on page 61. By default, the gateway does not use a SIM PIN.

Field	Description
IP Address Preference	This feature is only supported on the Verizon Wireless AirLink ES440. Use this field to select the preferred IP Address version. To use IPv6, it must be supported by your Mobile Network Operators and your account (SIM and APN). Options are: • IPv4—When the gateway connects to the mobile network, it is assigned only an IPv4 address. • IPv4 and IPv6 Gateway—When the gateway connects to the mobile network, it is assigned an IPv4 address and an IPv6 address. The IPv6 address and routing information are passed to the LAN clients so that they can acquire IPv6 addresses and pass IPv6 traffic over the mobile network. *Note: The LAN client must have IPv6 enabled and must be configured to use SLAAC (Stateless address auto configuration). The IPv6 address and routing information, and DNS servers are passed to the LAN clients via SLAAC.* *Note: Other than routing IPv6 packets between the WAN and the LAN, no other AirLink features are supported on IPv6.* The IP addresses are displayed on the Status > Home and Status > WAN screens.
Keep Alive (See Keep Alive on page 60.)	
Advanced *Note: Network credentials shown depend on the gateway, the radio module, and the network. Not all fields appear on all gateways. For details, see WAN/Cellular > Advanced on page 59.*	
CDMA Mobile IP	Mobile IP (MIP) Preferences. On a Mobile IP network, a device connects to the network using PPP. During the negotiation process the AirLink gateway is NOT required to present a username and password to authenticate because the authentication parameters are stored in the device itself. • Disabled, SIP only • MIP Preferred (Default)* • MIP Only *MIP is used when available with a fallback to SIP. *Note: Your account with your Mobile Network Operator or your location may not support all three of these options. check with your Mobile Network Operator as to which one should be used.*

Field	Description
Response to Incoming Ping	When a ping is received by the gateway from a remote location, the Response to Incoming Ping redirects it to the selected location. • No response: The incoming ping is completely ignored • ALEOS Responds (default): ALEOS returns to the Ping response. • Pass to Host: The ping is forwarded to the DMZ host with any response from the host forwarded back to the OTA location. If no host is connected, there is no ping response. *Note: Some Mobile Network Operators may block all ICMP traffic on their network. When ICMP is blocked by the operator, a ping sent to the gateway from a remote location is not received.*
LTE Authentication Mode	Specifies the authentication method to use when connecting to a mobile network Options are: • None • CHAP • PAP (default)
Network User ID	Network User ID The login that is used to login to the mobile network, when required. • Maximum 128 characters
Network Password	Network Password is the password that, when required, is used to login to the mobile network. • Maximum 30 characters
Network Watchdog Timer	Network Watchdog Timer If there is no WAN connection for the time configured in this field, the gateway reboots. Options are: • Disable—When this field and the Cellular Network Watchdog field are set to Disable, the gateway never reboots as a result of lack of network connectivity. • 5 Minutes • 10 Minutes • 15 Minutes • 30 Minutes • 45 Minutes • 1 Hour • 2 Hours (default) • 3 Hours • 4 Hours

Field	Description
Set Carrier (Operator) Selection	Manually specify an operator. Enter the desired parameters in the following format: mode[,format[,oper]] • mode= 0: Automatic—any affiliated operator [default] • mode= 1: Manual—use only the operator <oper> specified • mode= 4: Manual/Automatic—if manual selection fails, goes to automatic mode • format= 0: Alphanumeric (“name”) • format= 2: Numeric • oper=”name” See also +COPS and *NETOP? *Note: Not all operators or accounts allow specifying the operator. If the Mobile Network Operator doesn't support it, this command may appear to fail.*
Cellular Network Watchdog	Cellular Network Watchdog Options are: • Enable—When this Watchdog is enabled, the gateway reboots after several attempts to authenticate on the mobile network fail. (default) • Disable—When this field and the Network Watchdog Timer field are both set to Disable, the gateway never reboots as a result of lack of network connectivity.

Field	Description

LTE Active Reselection Interval	This feature assists the gateway to revert back to an LTE network if one becomes available.
	When an LTE AirLink gateway is connected to a non-LTE network, it may not hand over to an LTE network when one becomes available if data is being continuously transmitted or received.
	When the LTE Active Reselection Interval timer is configured, the AirLink gateway temporarily halts uplink data for the length of time configured in the LTE Reselection Time field if the gateway is connected to a non-LTE network. This allows the radio module to go idle and reconnect to an LTE network, if one is available.
	Note:
	• *If the LTE signal that the AirLink gateway receives is weaker than the HSPA+ signal, the gateway may not revert to LTE, depending on the local network characteristics.*
	• *This feature should be disabled:*
	  • *If the SIM in the gateway is not provisioned to work on an LTE network*
	  • *If the gateway is roaming*
	To use this feature:
	1. From the drop-down menu in the LTE Active Reselection Interval field, select how long the AirLink gateway is not on an LTE network before the reselection process begins. (Disabled is the default.)
	 
	2. Click Apply.
	3. Reboot the gateway.

LTE Reselection Time	Use this field to set how long the gateway radio should attempt to find and connect to an LTE network (i.e. how long the reselection process described in LTE Active Reselection Interval should last). Data for transmission during the reselection process is buffered. Options are: • 15 seconds • 20 seconds (default) • 25 seconds • 30 seconds
Current Radio Module Band	Band reported by the radio module as the one currently in use.

Field	Description

Always on connection	This field is intended for International gateways on the Vodafone network.
	This option allows you to configure the AirLink gateway to use minimal wireless network resources when there has not been any outgoing WAN network traffic.
	• Enabled—The AirLink gateway maintains a mobile network data connection. (default)
	• Disabled—Connect on traffic—The AirLink gateway only establishes a mobile network data connection:
	  • When there is network traffic
	  • If SMS Wakeup is configured and the gateway receives the specified type of SMS (For information on configuring SMS Wakeup, see SMS Wakeup on page 160.)
	*Note: You can also use AT*RADIO_CONNECT to switch the mobile network connection on and off. See *RADIO_CONNECT on page 295.*

Connection Timeout (minutes)	This field is intended for International gateways on the Vodafone network. This field only appears when Always on connection is set to Disable - Connect on traffic, and defines the timeout period for Always on connection. If there is no outgoing packet through the WAN interface during the period set in this field (in minutes), the AirLink gateway disables the WAN connection. This timer is triggered after every outgoing packet, except AT*IPPINGFORCE keep alive packets. • 2–65535 minutes (default is 2) *Note: You can also use AT*TRAFWUPTOUT to set the timeout period. See *TRAFWUPTOUT on page 296.*

Field	Description
Setting for Band (ES440 MC7700 and MC7710)	This feature enables advanced users to select the RF band range or technology the AirLink gateway uses. Most of the time it's best to leave this field at the default setting (All bands) but there may be times when you want to select a band range or technology that you know is more stable in the region where the AirLink gateway is located. The list of options displayed depends on the radio module in your gateway and its configuration. Possible options include: • All bands (default) • Europe 3G • North America 3G • Europe 2G • North America 2G • GSM ALL • Europe • North America • WCDMA ALL • LTE ALL *Note: For most users, it's best to leave the default setting (All bands). When this option is selected, your AirLink gateway connects to a the fastest network available. If you choose another option and the selected network is not available, the gateway will not be able to connect to the mobile network. For example, if you select LTE ALL and you are in an area where there is no LTE network available, the gateway will not be able to connect to a mobile network until you change this setting.*
Enable 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. Enabling 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: • Enable—MSS is clamped to the specified maximum value bi-directionally for all inbound (remote-to-LAN) and outbound (LAN-to-remote) TCP connections when the TCP session is established using the cellular interface. • Disable (default)
Maximum Segment Size - MSS (bytes)	When MSS Clamping is enabled, set the Maximum TCP Segment Size • 256–1460 bytes (default is 1460)
APN Backup (See Backup APN on page 64.)	
Bandwidth Throttle (See Bandwidth Throttle on page 65.)	
Re-Activation (See Re-Activation on page 64.)	

Table 4-1: WAN/Cellular > Network Credentials

Field	Gateway and Radio Module[a]	
	ES440 (MC7750)	ES440 (MC77x0)
APN in Use		✔
LTE Data Service	✔	

a. To determine the radio module for your gateway, in ACEmanager, go to Status > About.

Table 4-2: WAN/Cellular > Advanced

Field	Gateway and Radio Module[a]	
	ES440 (MC7750)	ES440 (MC77x0)
CDMA Mobile IP	✔	
Network Roaming Preference	✔	
Setting for Band		✔
Network Authentication Mode		✔
Current Radio Module Band		✔

a. To determine the radio module for your gateway, in ACEmanager, go to Status > About.

Keep Alive

If the AirLink gateway does not receive a valid packet for a specified time, Keep Alive tests the connection to the mobile network by pinging a configured IP address. Keep Alive is only recommended if you have a remote terminated device that infrequently communicates to the network or if you have experienced issues over time where the device can no longer be reached remotely.

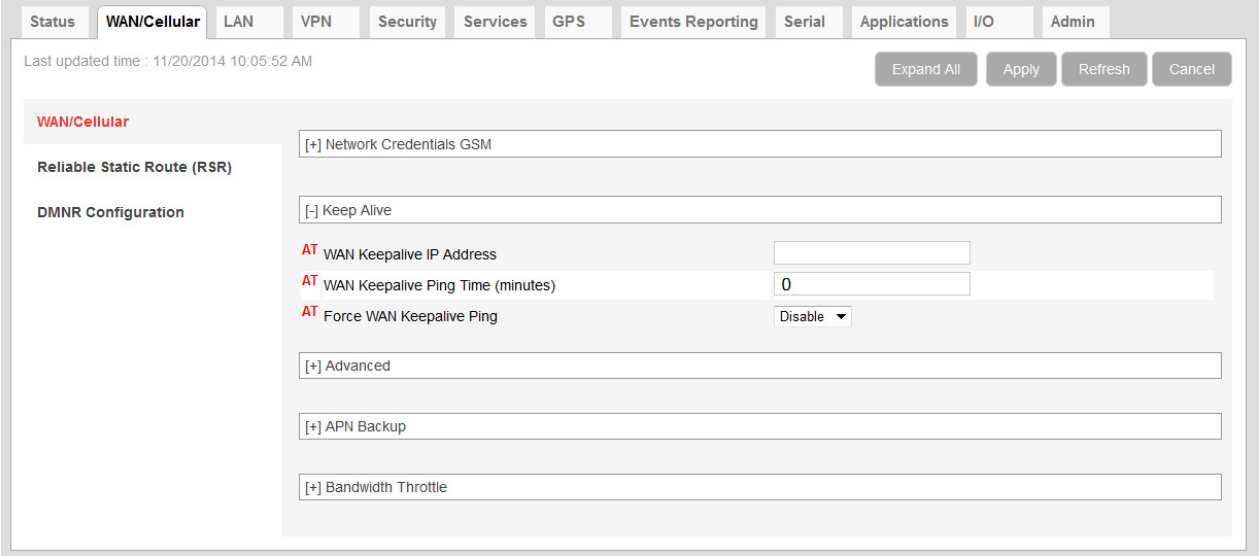


Figure 4-2: ACEmanager: Wan/Cellular > Keepalive

Field	Description
WAN Keepalive IP Address	The IP address that the AirLink gateway pings to determine if there is Internet connectivity and to make sure the IP address is accessible. Enter the IP address or fully qualified domain name for the AirLink gateway to ping to keep itself alive (online). Options are: • IP address • Domain name You can also use *IPPINGADDR to set this parameter.

Field	Description
WAN Keepalive Ping Time (minutes)	The amount of time the AirLink gateway goes without receiving a valid packet before the first Keepalive ping is sent. Options are: • 0—Disable Keepalive ping (default) • 1–255 minutes Most applications work well with an interval of 15 to 60 minutes. If the first ping fails, the AirLink gateway sends four additional pings. If all five pings fail, the AirLink gateway reboots. After rebooting, the AirLink gateway waits 60 minutes before sending another Keepalive ping (regardless of the setting in this field). This prevents frequent rebooting (based on the Keepalive Ping Time setting) if the IP address used for the Keepalive ping is not accessible. *Note: Using Keepalive ping may accrue data charges. Each individual ping is approximately 98 bytes (196 bytes for ping sent plus ping response).* You can also use *IPPING to set this parameter.
Force WAN Keepalive Ping	Determines if the ping should be sent even if IP traffic is received during the Keepalive ping interval. Options are: • Disable (default) • Enable If the first ping fails, the AirLink gateway sends four additional pings. If all five pings fail, the AirLink gateway reboots. After rebooting, the AirLink gateway waits 60 minutes before sending another Keepalive ping (regardless of the setting in this field). This prevents frequent rebooting (based on the Keepalive Ping Time setting) if the IP address used for the Keepalive ping is not accessible. You can also use *IPPINGFORCE to configure this parameter.

SIM PIN

If you have a SIM card with a PIN configured, you can configure ALEOS to enter the PIN on reboot, so human intervention is not required.

This feature has two requirements:

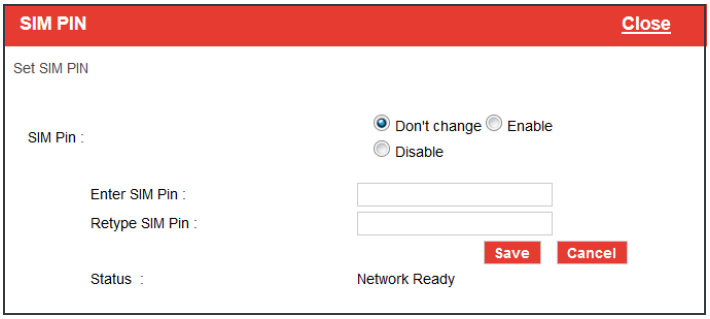
- A PIN-locked SIM card—Contact your Mobile Network Operator to ensure that they support this feature and to obtain a PIN-locked SIM card and PIN.
- The SIM PIN feature in ACEmanager must be enabled. See Enable the SIM PIN.

If the AirLink gateway has a PIN-locked SIM installed and this feature is not enabled in ACEmanager, the AirLink gateway is unable to go on air and the Network Status field on the Status > Home screen displays the message “SIM PIN incorrect, # attempts left”.

Enable the SIM PIN

To enable the SIM PIN in ALEOS:

1. In ACEmanager, go to WAN/Cellular.
2. Click the SIM PIN button. The following pop-up window appears.



3. Select Enable.
4. Enter the PIN (obtained from your Mobile Network Operator) twice and click Save.
5. Reboot the AirLink gateway.

After rebooting:

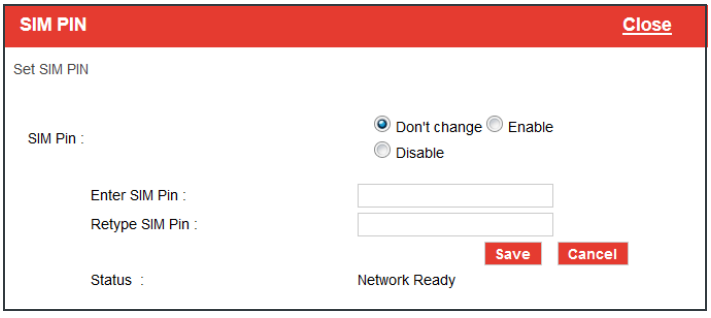
- The AirLink gateway uses the configured PIN on subsequent re-boots.
- The SIM PIN pop-up window shows the default settings. Don't change is selected and the SIM PIN fields are blank. "Don't change" indicates that the PIN is used in the same way on every boot.

Note: If you enter an incorrect PIN, the AirLink gateway is unable to go on air, and the Network Status field on the Status > Home screen displays "SIM PIN incorrect, # attempts left". The failed PIN is not retried on subsequent reboots to prevent exhausting the available number of retries with repeated attempts with an incorrect PIN.

Change the SIM PIN

To change the SIM PIN:

1. In ACEmanager, go to WAN/Cellular.
2. Click the SIM PIN button. The following pop-up window appears.



3. Select Enable.
4. Enter the new PIN twice and click Save.
5. Reboot the AirLink gateway.

After rebooting:

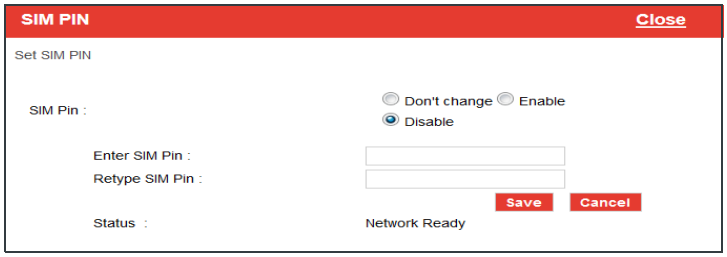
- The AirLink gateway uses the configured PIN on subsequent re-boots.
- The SIM PIN pop-up window shows the default settings. Don't change is selected and the SIM PIN fields are blank. "Don't change" indicates that the PIN is used in the same way on every boot.

Note: If you enter an incorrect PIN, the Network Status field on the Status > Home screen displays "SIM PIN incorrect, # attempts left". The failed PIN is not retried on subsequent reboots to prevent exhausting the available number of retries with repeated attempts using an incorrect PIN.

Disable the SIM PIN

To disable the SIM PIN:

1. In ACEmanager, go to WAN/Cellular.
2. Click the SIM PIN button. The following pop-up window appears.



3. Select Disable.
4. Enter the PIN twice and click Save.
   If you enter an incorrect PIN or no PIN, the feature will not be disabled.
5. Reboot the AirLink gateway.

After rebooting:

- The AirLink gateway no longer uses the stored PIN on subsequent re-boots.
- The SIM PIN pop-up window shows the shows the feature is Disabled.

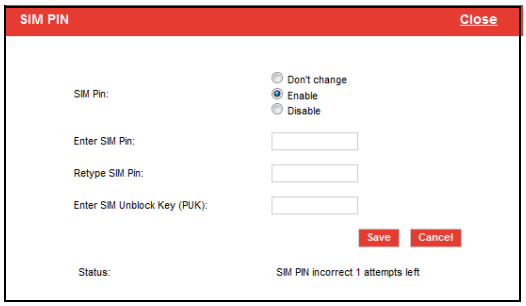
Unblocking a SIM PIN

When you enable, change or disable a SIM PIN, you have a set number of attempts to enter the correct PIN, depending on your Mobile Network Operator. If the correct PIN is not entered in the alloted number of attempts, the SIM PIN becomes blocked and you need a PUK code to unblock it.

To unblock a SIM PIN:

1. Contact your Mobile Network Operator to obtain a PUK code.
2. In ACEmanager, go to WAN/Cellular.
3. Click the SIM PIN button.

When the PIN is blocked, an additional field (Enter SIM Unblock Code) appears.



4. Select Enable.
5. Enter the new PIN code.
6. Enter the PUK and click Save.

   Be careful when entering the PUK. You have a limited number of attempts to enter the correct PUK (generally 10) before the SIM card is disabled. If the PUK does not unblock the SIM PIN after the first few attempts, contact your Mobile Network Operator.

   If you have exhausted all the alloted attempts to enter the correct PUK, the Mobile Network Operator may give you a new SIM card, or a new code to enable your existing SIM card. AirLink products do not support this type of code. To enter the code:

   a. Remove the SIM card from your AirLink gateway (following the instructions in the AirLink gateway Hardware User Guide) and insert it in a cell phone that accommodates a MiniSIM (2FF) card.

   b. Enter a new code provided by the Mobile Network Operator and then return the SIM card to the AirLink gateway.

Re-Activation

The Re-Activation section of the WAN/Cellular tab only appears for EV-DO/1X gateways. The Re-Activation feature can only be used when a particular gateway that has already been activated needs re-activation. If your gateway needs to be reactivated, click the button labeled “Re-Activate Cellular Account”. When you click this button, the status shows the progress of the re-activation.

Note: If the provision fails, an error message appears.

After the provision process finishes, the system then restarts, as a reset is necessary to initiate the new account information.

Backup APN

This feature enables you to configure a backup APN to be used as a backup network connection mechanism, only if the primary APN is not available. When it is enabled, the gateway connects to the backup APN only if it is unable to connect to the primary APN.

Note: Switching to the backup APN can take five minutes or more, depending on the gateway. If the gateway is always connecting to the backup APN, check the primary APN to ensure that it is configured correctly.

To configure a backup APN:

1. Go to WAN/Cellular > APN Backup.

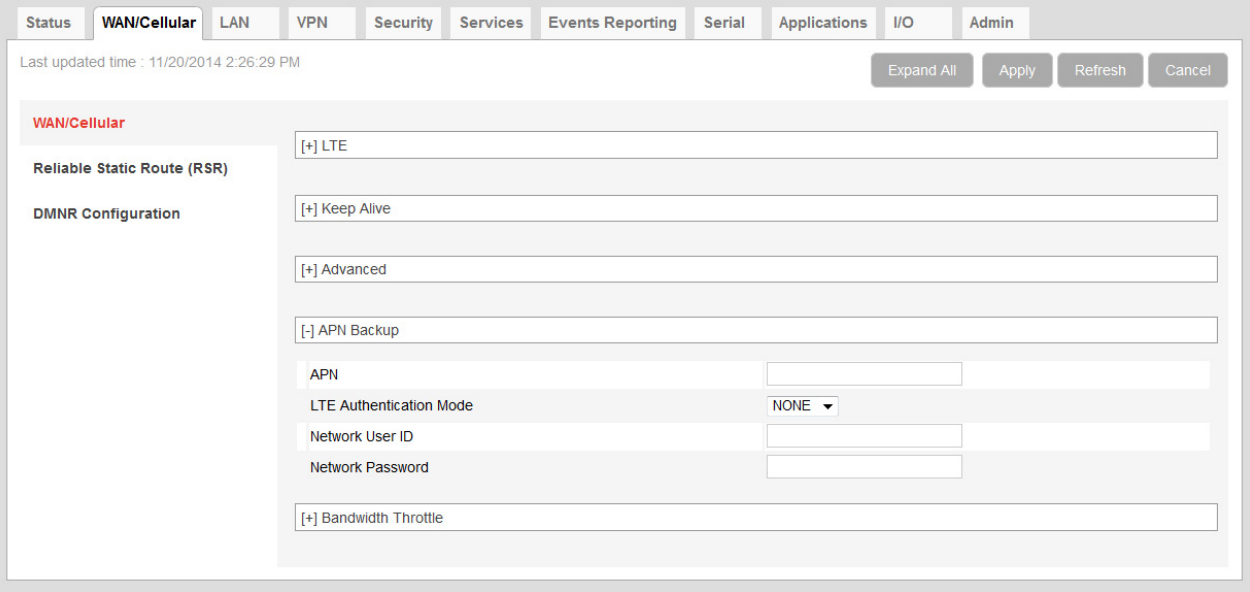


Figure 4-3: ACEmanager: WAN/Cellular > APN Backup

2. Enter the backup APN (maximum 100 characters).
3. Select the Network Authentication Mode. The options are:
   - PAP (default)
   - CHAP
   - NONE
4. Enter the Network User ID and Password, if these are required for the wireless network.
5. Click Apply.

Bandwidth Throttle

This feature helps you manage your data account by allowing you to configure the AirLink gateway to restrict the real-time available bandwidth. You can:

- Place limits on the uplink traffic, downlink traffic, or both
- Allow for burst of traffic on the uplink, downlink, or both, while still maintaining the over-all desired bandwidth limit

Traffic that exceeds the limits is dropped. Status fields keep running tallies of data sent and received and the number of uplink and downlink packets dropped.

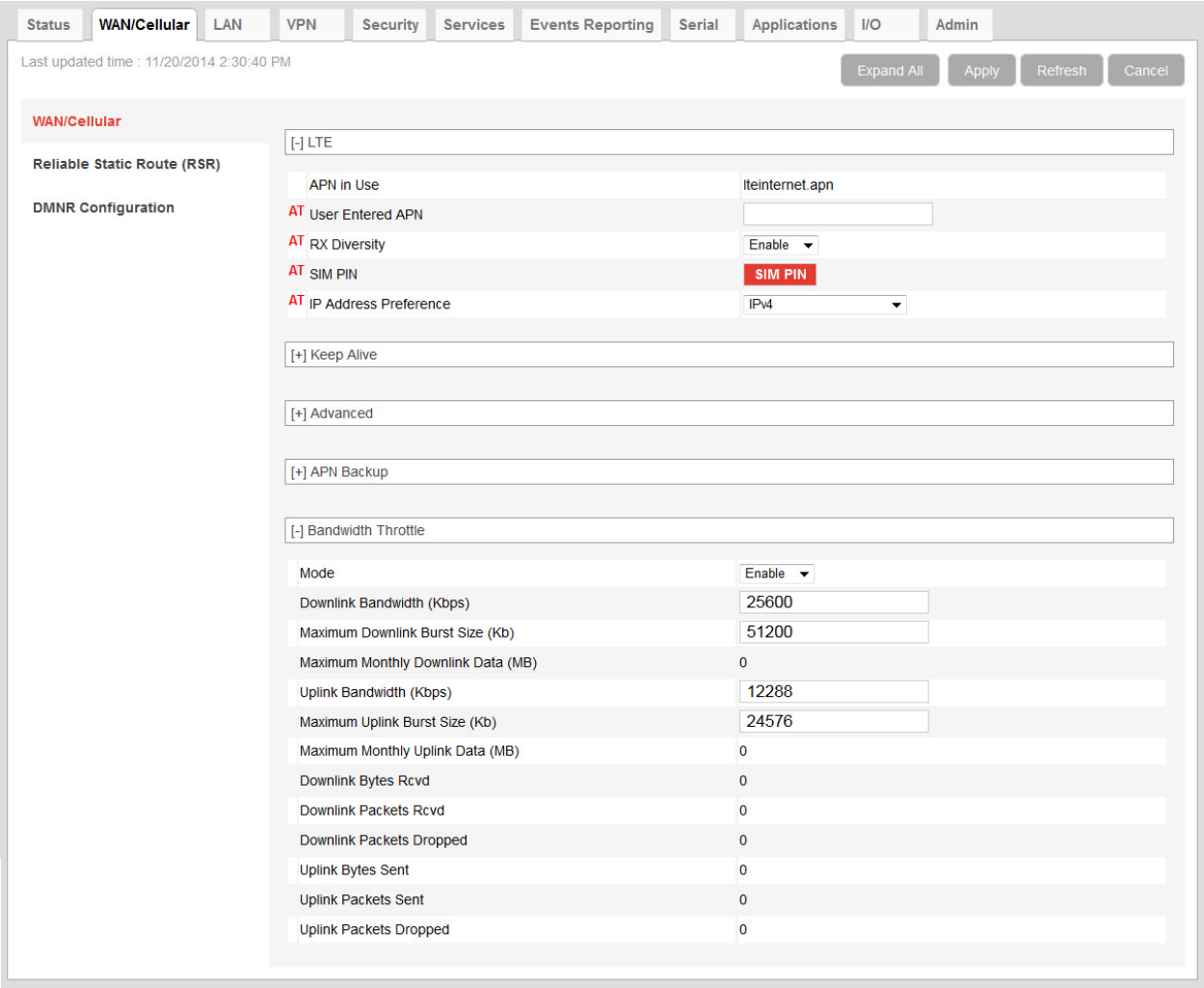


Figure 4-4: ACEmanager: WAN/Cellular > Bandwidth Throttle

Field	Description
Bandwidth Throttle	
Mode	Allows you to Enable or Disable the feature Default is Disable.
Downlink Bandwidth (Kbps)	The maximum downlink bandwidth in Kilobits per second (Kbps) This is the long-term bandwidth limit. Options are: • 0–512000 (500 Mbps) Default is 25600. 0 = feature disabled for downlink traffic

Field	Description
Maximum Downlink Burst Size (Kb)	Maximum size for bursts of downlink traffic in Kilobits (Kb) This field allows the AirLink gateway to handle temporary bursts of downlink traffic without dropping packets. When the actual downlink traffic is less than the value configured in the Downlink Bandwidth (Kbps) field, ALEOS collects credits that can be used for bursty traffic. The value in this field is the maximum amount of credit that can be collected. Options are: • 64–512000 (500 Mb) Default is 51200. *Note: Sierra Wireless recommends that the Maximum Downlink Burst Size be set at 2x the value configured in the Downlink Bandwidth (Kbps) field. If the Maximum Downlink Burst Size is set at more than 60x the value configured in the Downlink Bandwidth (Kbps) field, the bandwidth throttle feature is disabled for downlink traffic.*
Maximum Monthly Downlink Data (MB)	An estimate of the maximum monthly downlink data in Megabytes (MB), based on the value set in the *Downlink Bandwidth (Kbps)*. Maximum monthly downlink data (MB) = Downlink bandwidth × 2592000 ÷ 8192 Where: 2592000 is the number of seconds in a month (30 days/month) 1 MB = 1024 KB; 1024 × 8 = 8192 Kb/MB
Uplink Bandwidth (Kbps)	The maximum uplink bandwidth in Kilobits per second (Kbps) This is the long-term bandwidth limit. Options are: • 0–204800 (200 Mbps) Default is 12288. 0 = feature disabled for uplink traffic
Maximum Uplink Burst Size (Kb)	Maximum size for bursts of uplink traffic in Kilobits (Kb) This field allows the AirLink gateway to handle temporary bursts of uplink traffic without dropping packets. When the actual uplink traffic is less than the value configured in the Uplink Bandwidth (Kbps) field, ALEOS collects credits that can be used for bursty traffic. The value in this field is the maximum amount of credit that can be collected. Options are: • 32–204800 (200 Mb) Default is 24576. *Note: Sierra Wireless recommends that the Maximum Uplink Burst Size be set at 2x the value configured in the Uplink Bandwidth (Kbps) field. If the Maximum Uplink Burst Size is set at more than 60x the value configured in the Uplink Bandwidth (Kbps) field, the bandwidth throttle feature is disabled for uplink traffic.*
Maximum Monthly Uplink Data (MB)	An estimate of the maximum monthly uplink data i in Megabytes (MB), based on the value set in the *Uplink Bandwidth (Kbps)* Maximum monthly uplink data (MB) = Uplink bandwidth × 2592000 ÷ 8192 Where: 2592000 is the number of seconds in a month (30 days/month) 1 MB = 1024 KB; 1024 × 8 = 8192 Kb/MB
Downlink Bytes Rcvd	Number of downlink bytes received The value is updated every 30 seconds, and is reset to zero on gateway reboot or reset to factory default settings.

Field	Description
Downlink Packets Rcvd	Number of downlink packets received The value is updated every 30 seconds, and is reset to zero on gateway reboot or reset to factory default settings.
Downlink Packets Dropped	Number of downlink packets dropped because the limits set in Downlink Bandwidth (Kbps) and Maximum Downlink Burst Size (Kb) have been exceeded The value is updated every 30 seconds, and is reset to zero on gateway reboot or reset to factory default settings.
Uplink Bytes Sent	Number of uplink bytes sent The value is updated every 30 seconds, and is reset to zero on gateway reboot or reset to factory default settings.
Uplink Packets Sent	Number of uplink packets sent The value is updated every 30 seconds, and is reset to zero on gateway reboot or reset to factory default settings.
Uplink Packets Dropped	Number of uplink packets dropped because the limits set in Uplink Bandwidth (Kbps) and Maximum Uplink Burst Size (Kb) have been exceeded The value is updated every 30 seconds, and is reset to zero on gateway reboot or reset to factory default settings.

Reliable Static Routing (RSR)

Reliable Static Routing enables you to force specified traffic to use different routing rules (rather than the default, which is usually cellular) to direct specified traffic (from or to either the AirLink gateway or a connected device) to a designated primary route. If the primary route fails, the specified traffic uses a backup route.

First, you designate specific traffic to use the primary route, based on the destination IP address and subnet mask. A configured Tracking Object Test verifies the validity of the primary route. If the test fails, the backup route is used. The Tracking Object Test continues to run and as soon as it returns a “Pass”, traffic is switched back to the primary route.

You can direct the traffic to a network (Figure 4-5) or to an individual host (Figure 4-6).

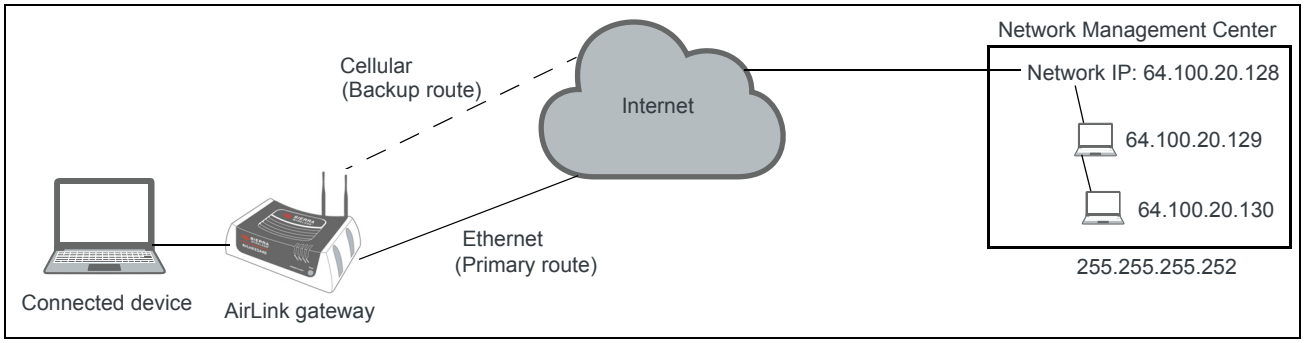


Figure 4-5: RSR directed to a destination network

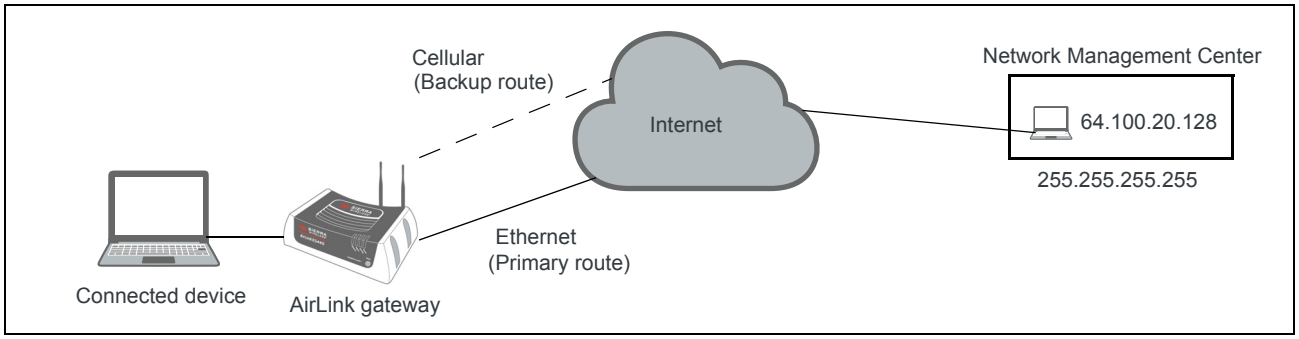


Figure 4-6: RSR directed to a destination IP address (individual host)

In a business continuity application where the router also has a routable IP address from a wireline gateway connection (as shown in Figure 4-7) the IT administrator may prefer to use that lower cost connection for data sourced from the AirLink gateway, such as SNMP or AVMS data. When reliable static routing is configured, the Tracking Object tests the validity of the primary route and data from the AirLink gateway is transmitted through the primary route (in this example, the wireline connection). If the tracking object determines that the primary route is down, data is transmitted through the backup (in this example, the wireless connection).

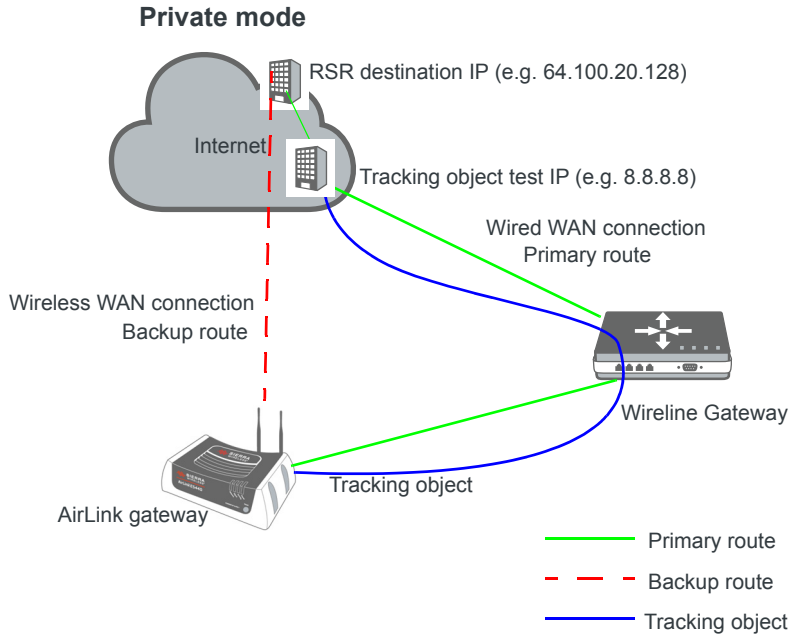


Figure 4-7: Private Mode with Reliable Static Routing

Sierra Wireless recommends a Private Mode network as the most reliable configuration to use in a business continuity failover application as defined in the AirLink Hardware User Guide (or Figure 4-7) with Reliable Static Routing and Reverse Telnet. For more information, see Private and Public Mode on page 79.

To configure Reliable Static Routing:

1. Connect the hardware as shown in Figure 4-7.

2. Use the Tracking Object to test the connection:
   a. In ACEmanager, go to WAN/Cellular > Reliable Static Route (RSR).

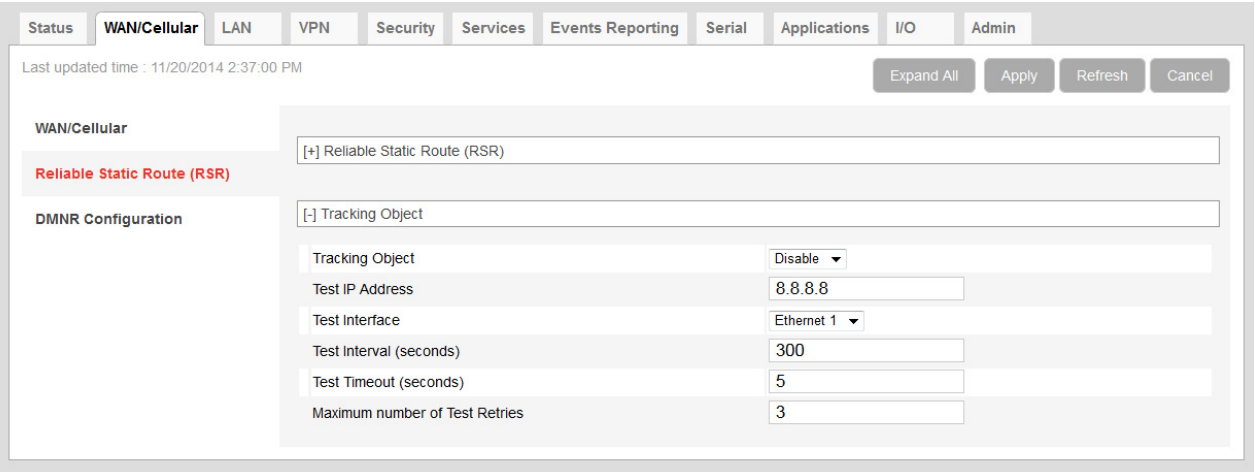


Figure 4-8: ACEmanager: WAN/Cellular > Reliable Static Route (RSR), Tracking Object

   b. Under Tracking Object, enter the Test IP address, using a host behind the gateway that has a reliable IP address, such as 8.8.8.8.
   c. From the drop-down menu, select Ethernet 1 as the Test Interface.
   d. Leave the default values for the Test Interval, Test Timeout, and Maximum number of retries.
   e. In the Enable/Disable Tracking Object field, select Enable.
   f. Click Apply.
   g. The Tracking Object pings the Test IP address configured in step b. In ACEmanager go to Status > WAN/Cellular and note the result in the RSR Test Result field.
3. Disable Tracking Object.

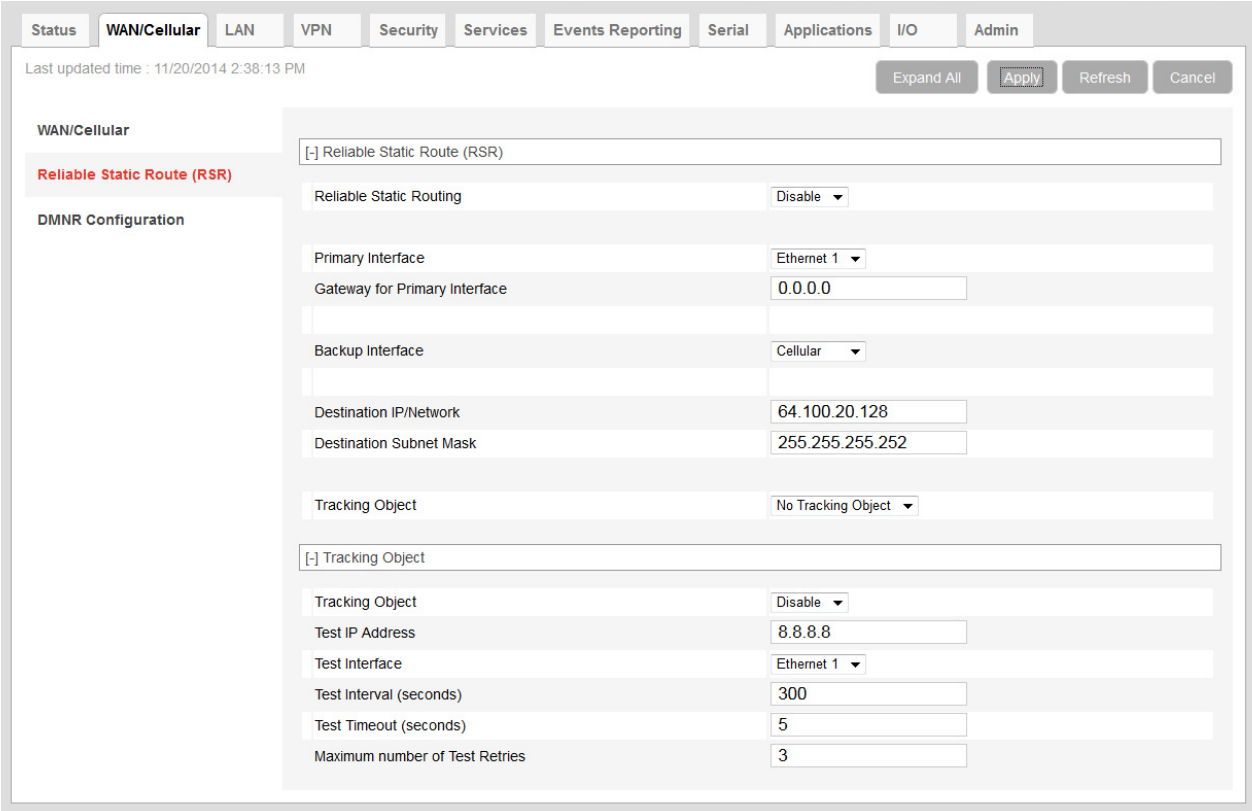


Figure 4-9: ACEmanager: WAN/Cellular > Reliable Static Route (RSR)

Note: Configure all the other fields before setting the Enable/Disable Reliable Static Routing field. Once you enable RSR, some fields on this page are not editable.

4. Select the interfaces for the primary and backup routes. The options are:
   - Ethernet 1 (default for primary route)
   - USB
   - Cellular (default for backup route)

   If you select Ethernet 1, you are given the option to enter a gateway IP address that is used as the next hop for reaching the destination network.[1]



   - If the Tracking Object test completed in step 2 was successful, leave this field at the default value (0.0.0.0).
   - If the Tracking Object test completed in step 2 failed, enter the gateway IP address in this field.

5. Set the Destination IP/Network and Destination Subnet Mask.

   To configure the RSR destination as a network, as shown in Figure 4-9, you would enter:

1. This applies to both the Primary and the Backup interface.

- 64.100.20.128 in the Destination IP/Network field.
- 255.255.255.252 in the Destination Subnet Mask field.

To configure the RSR destination as an individual host, as shown in Figure 4-9, you would enter:

- 64.100.20.128 in the Destination IP/Network field.
- 255.255.255.255 in the Destination Subnet Mask field.

6. Set the Tracking Object (Tracking Object 1 or No Tracking Object). Normally, you would select Tracking Object 1 from the drop-down menu.
7. Under Tracking Object, leave the Enable/Disable Tracking Object set at Disable until you finish configuring the other Tracking Object fields.
8. Enter the Test IP address (normally an IP address within the Traffic Selection Criteria Network/Subnet).
9. From the drop-down menu, select the desired Test Interface (normally the same interface as the primary route). Options are:
   - Ethernet 1
   - USB
   - Cellular
10. Enter the Test Interval in seconds. This is the interval between Tracking Object Tests.

    For most applications, the default values for the Test Interval, Test Timeout, and Maximum number of retries should be fine.

    If you want to change these values, be aware of the following:
    - Selecting a short test interval increases network traffic and may lead to false failures if the network is busy.
    - Selecting a long test interval may mean that traffic does not switch to the secondary route quickly enough when the primary route fails.
    - The test interval must be greater than the product of Test Timeout × Maximum number of Test Retries.
      [Test Interval] > [Test Timeout] × [Maximum number of Retries]
11. Enter the Test Timeout in seconds. This is the time to wait for a response. If this time expires before a response is received, the test attempt fails.
12. Enter the Maximum number of Test Retries. If the first Tracking Object Test fails, this is the number of times the gateway sends additional test messages (without receiving a response) before it declares the test as failed and switches the specified traffic to the backup network.
13. In the Enable/Disable Tracking Object field, select Enable.
14. In the Enable/Disable RSR field, select Enable.

Go to Status > WAN/Cellular to check the RSR Test Result and confirm that traffic is being sent through the primary route. If the RSR Test Result field indicated that the Tracking Object Test has failed, validate the connectivity of the primary path. (The test result of Unknown indicates that the test has not yet run.)

Dynamic Mobile Network Routing (DMNR)

Note: DMNR is supported only on the Verizon Wireless network.

DMNR provides direct communication between customer sites (for example, between remote subnets and the corporate data center) through a Mobile Network Operator's (MNO's) private network (isolated from Internet traffic).

DMNR creates a tunnel between the home agent on the MNO's private network and the AirLink gateway.

Note: Primary Access Mode DMNR is supported only on Ethernet LANs.

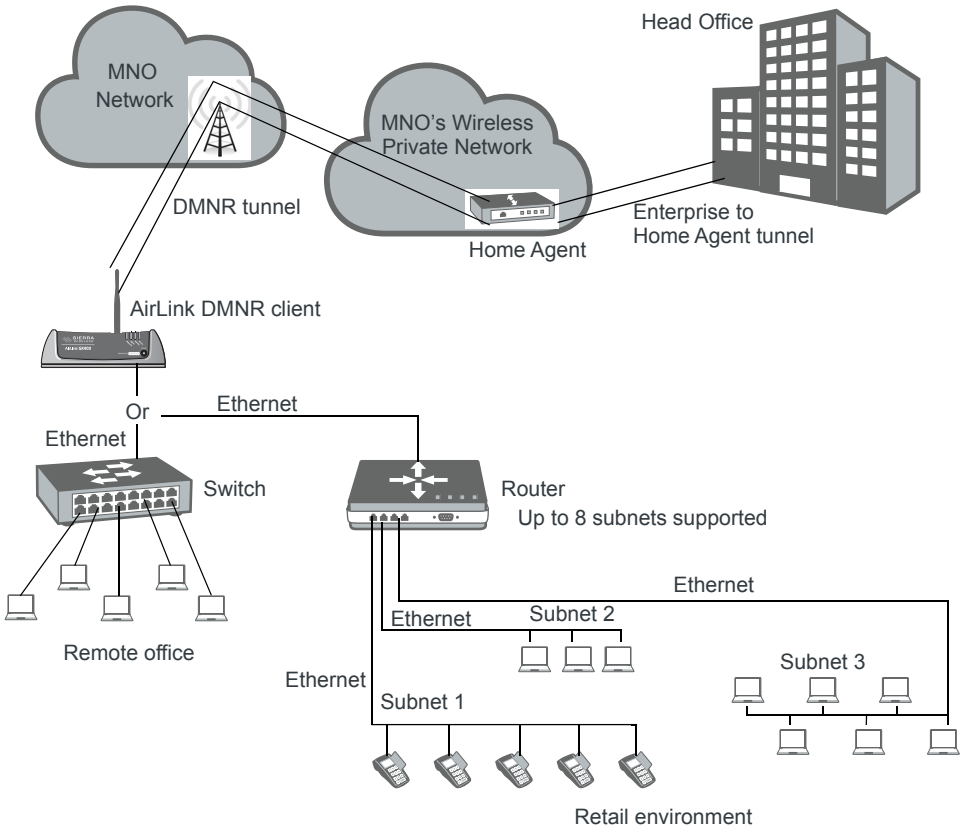


Figure 4-10: DMNR Configuration

Before configuring DMNR:

1. Go to LAN > DHCP/Addressing and ensure that the Host Connection Mode is set to All Hosts Use Private IPs (default).
2. Go to LAN > Host Port Routing and set the Primary Gateway field to Disable.
3. Go to VPN and disable any VPNs you have set up.

   Once DMNR is configured, all traffic from the connected LANs goes through the DMNR tunnel.
4. Go to Security > Port Forwarding and set the DMZ Enabled field to Disable.
5. Reboot the gateway.

Note: For the DMNR registration process to complete successfully, there must be a switch, router, or other device physically connected to the AirLink gateway's Ethernet port.

To configure DMNR:

1. Go to WAN/Cellular > DMNR Configuration.

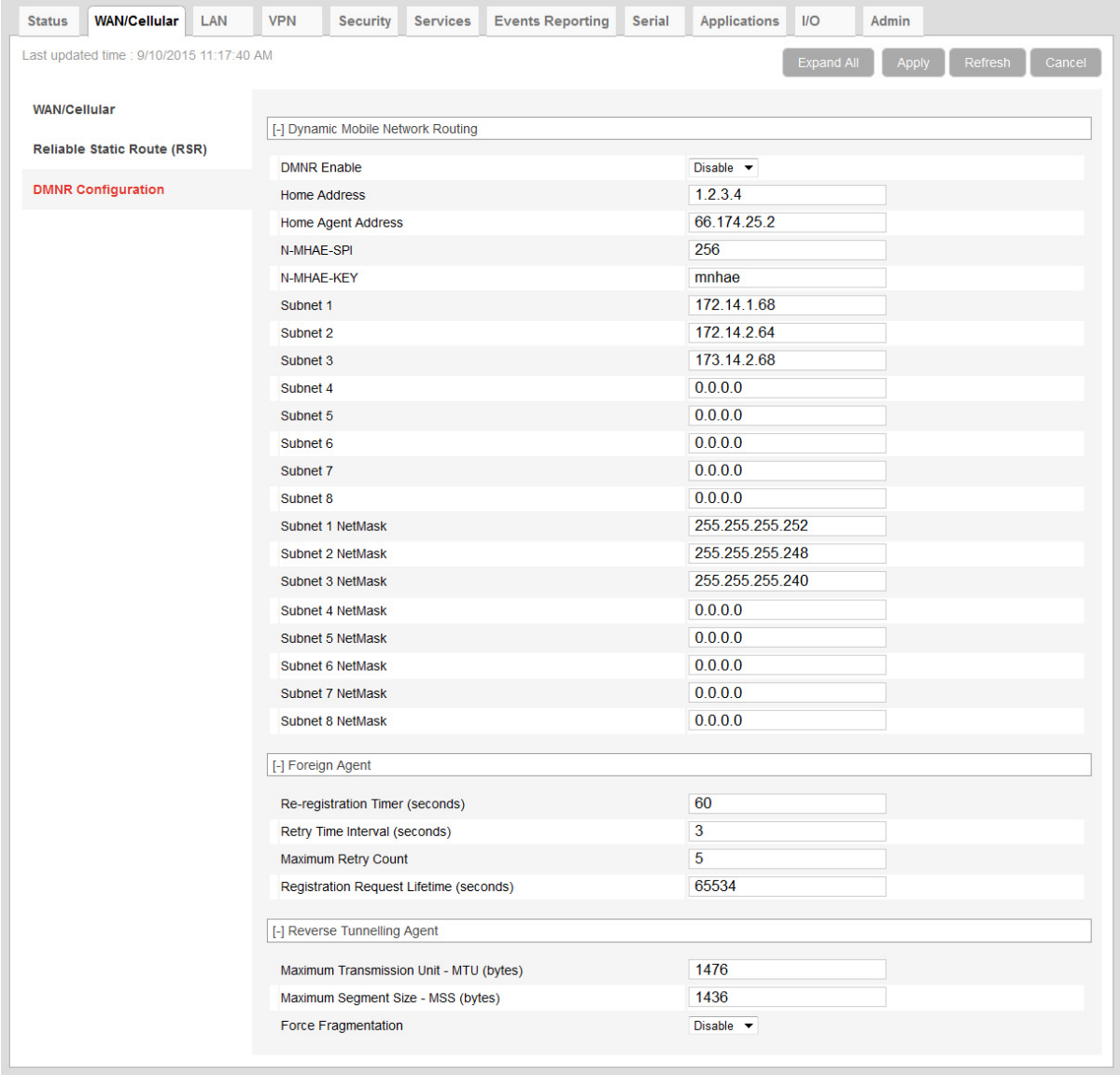


Figure 4-11: ACEmanager: WAN/Cellular > DMNR Configuration

2. Configure the fields as outlined in the following table.

Field	Description
Dynamic Mobile Network Routing	
DMNR Enable	Enables Dynamic Mobile Network Routing. Options are: • Enable • Disable (default)[a] *Note: Configure all the other parameters first and then set this field to Enable. When this field is set to Enable, the other fields in this window are read-only.*
Home Address	Enter a home address for the AirLink gateway. This address is used to distinguish the AirLink gateway used for DMNR. You can enter any IP address for the Home Address, but if you are using more than one AirLink gateway for DMNR, each must have a different home address. Suggested value is 1.2.3.4. This field cannot be left blank.
Home Agent Address	IP address of the Home Agent (available from your Mobile Network Operator)
N-MHAE-SPI	NEMO Authentication Extension Security Parameter Index (available from your Mobile Network Operator)
N-MHAE-KEY	NEMO Authentication Extension Key (available from your Mobile Network Operator)
Subnet 1 – 8	Enter the IP addresses for the subnets you want to include in the DMNR network. You can configure up to 8 subnets. 0.0.0.0 indicates that the subnet is not configured. *Note: If you want to remove a subnet from the DMNR configuration, replace the IP address with 0.0.0.0 rather than deleting it.*
Subnet 1 – 8 NetMask	Enter the Subnet Masks for the subnets you want to include in the DMNR network. 0.0.0.0 indicates that the subnet mask is not configured. *Note: If you want to remove a subnet mask from the DMNR configuration, replace the IP address with 0.0.0.0 rather than deleting it.*

a. If you disable DMNR when the DMNR tunnel is up, no disconnect message is sent, resulting in a temporary mismatch between the reachability of the (NEMO) subnets on the gateway and the Home Agent.

3. Click the + beside Foreign Agent and Reverse Tunnelling Agent.
4. Configure the Foreign Agent and Reverse Tunnelling Agent.

Field	Description
Foreign Agent	
Re-registration Timer (seconds)	The frequency with which the foreign agent re-registers its subnets • If the registration status is Down, the foreign agent re-registers its subnets when the time configured in this field expires. • If the registration status is Up, the frequency with which the foreign agent re-registers its subnets is equal to the Registration Response Lifetime minus the value configured in this field. The Registration Response Lifetime is usually equal to the Registration Request Lifetime (seconds). Once you have enabled DMNR, you can confirm the Registration Response Lifetime in ACEmanager (see Figure 4-12 on page 77). Options are: • 1–60 seconds (Default is 60 seconds.)
Retry Time Interval (seconds)	The interval (in seconds) between retries if the re-registration fails. Options are: • 1–5 seconds (Default is 5 seconds.)
Maximum Retry Count	Maximum number of re-registration tries allowed. Options are: • 0–5 (Default is 3.)
Registration Request Lifetime (seconds)	Enter the desired registration lease time (in seconds). Options are: • 0–65534 seconds (Default is 65534.)
Reverse Tunnelling Agent	
Maximum Transmission Unit - MTU (bytes)	Use this field to set the tunnel MTU for packets sent over the DMNR/GRE tunnel. Note that the tunnel adds 24 bytes to each packet so the tunnel MTU should be set at least 24 bytes lower than the Mobile Network MTU in order to avoid packet fragmentation. Options are: • 576–1500 (Default is 1476.)
Maximum Segment Size - MSS (bytes)	Use this field to set the TCP maximum segment size for the packets (in bytes). Options are: • 68–1436 (Default is 1436.)
Force Fragmentation	Allows you to override the “Do not fragment” bit in the incoming packet header and send large packets through the DMNR tunnel Options are: • Enable—The “Do not fragment” bit in incoming packet header is cleared. This setting is useful if you need to send large packets or you do not know the MTU of all the routers in the network path. • Disable—The “Do not fragment” bit in the incoming packet header is respected. If the bit is set, packets larger than the MTU are dropped. If the DF bit is clear, packets larger than the MTU are fragmented and sent. (Default)

5. In the DMNR Enable field, select Enable.

   Once DMNR is enabled, the fields are read-only. If you want to change any of the field entries, set the DMNR Enable field to Disable, make the required change, and then set the field to Enable.

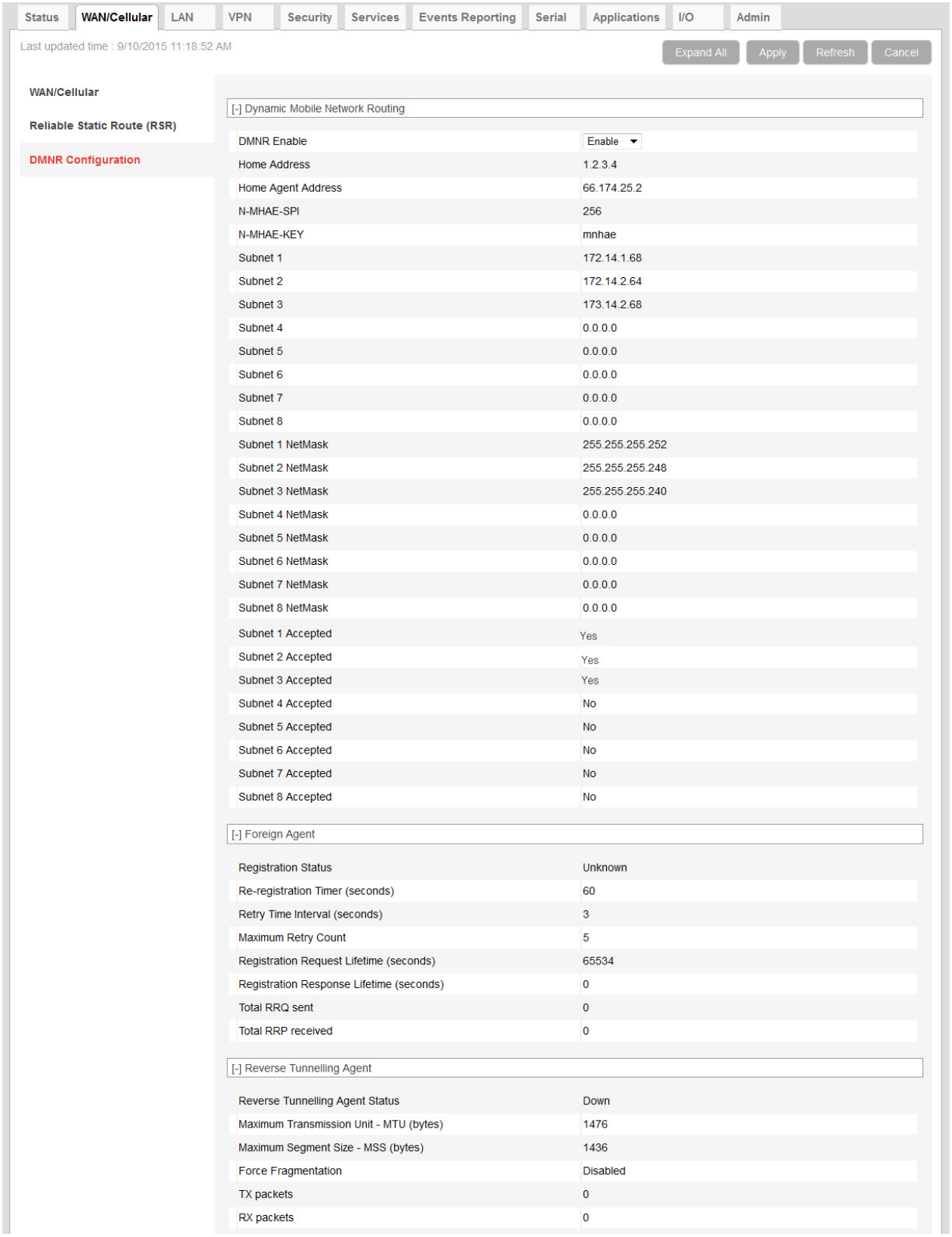


Figure 4-12: ACEmanager: WAN/Cellular > DMNR Enabled

Once DMNR is enabled, additional status fields appear, as described in the following table.

Field	Description
Dynamic Mobile Network Routing	
Subnet 1–8 Accepted	Confirms that the subnet configuration is accepted. Options displayed are: • Yes—The subnet is configured and accepted. • No—The subnet is not configured or not accepted.
Foreign Agent	
Registration Status	Foreign agent registration status Options displayed are: • Pass—A response has been received form the Home Agent • Fail—No response from the Home Agent • Unknown—Initial state
Registration Response Lifetime (seconds)	Shows the length of the current lease time (in seconds).
Total RRQ sent	Number of Registration Requests sent
Total RRP received	Number of Registration Responses received
Reverse Tunnelling Agent	
Reverse Tunnelling Agent Status	DMNR tunnel status This field only appears when DMNR is enabled. Options displayed are: • Up—DMNR tunnel is up. • Down—DMNR tunnel is down.
Force Fragmentation	Status of the Force Fragmentation field • Enabled • Disabled For more information, see Force Fragmentation on page 76.
TX packets	Number of packets transmitted The counter is reset when: • DMNR is disabled. • When the DMNR tunnel (Reverse Tunnelling Agent Status) is down.
RX packets	Number of packets received The counter is reset when: • DMNR is disabled. • When the DMNR tunnel (Reverse Tunnelling Agent Status) is down.

5: LAN Configuration

You can use the AirLink gateway to route data between one or more connected devices and the Internet via the mobile network. The AirLink gateway has two modes you can use for configuring a LAN—Private Mode and Public Mode.

Private and Public Mode

Private Mode and Public Mode are Sierra Wireless terms. In Private Mode, the router or laptop connected to the AirLink gateway has a LAN IP address. In Public Mode the AirLink gateway passes the WAN IP address to the router or laptop. Figure 5-1 shows the two types of configurations.

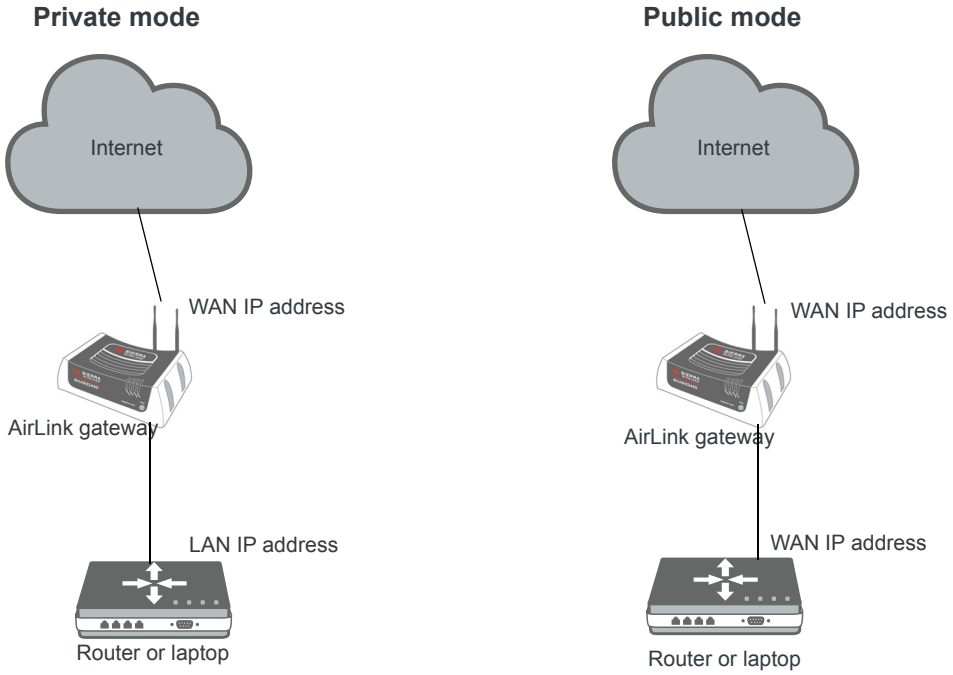


Figure 5-1: Private vs. Public Mode

Private Mode

Private Mode uses Network Address Translation (NAT) to enable the non-routable device to access the Internet. Data from the connected devices is passed through the AirLink gateway. By default, the first connected Ethernet or USBnet host is the DMZ host.

Public Mode

Public Mode is similar to IP pass-through. When Public Mode is enabled, by default the Public Mode host becomes the DMZ host. Public Mode is required when the connected device needs a routable IP address and has no other connection to obtain it.

Tip: *When using Public Mode, Sierra Wireless recommends connecting the AirLink gateway directly to the computer or other end device. Using a hub or switch may prevent the AirLink gateway from updating the IP address of the end device when an IP address is received from the mobile network.*

Port Use

Applications running on a LAN client such as a router or laptop must use different ports from those used by ALEOS features on the AirLink gateway. For a list of inbound ports used by ALEOS, see Inbound Ports Used by ALEOS on page 342.

DHCP/Addressing

This section is primarily a status display of the configurations, with a few options that are global to all interface types. Interfaces that are enabled in the current configuration are displayed with their configured settings.

DHCP addresses and subnets are assigned to the LAN side interfaces display.

Note: If the gateway has not been reset since configuration changes were made, the current configuration in use may be different.

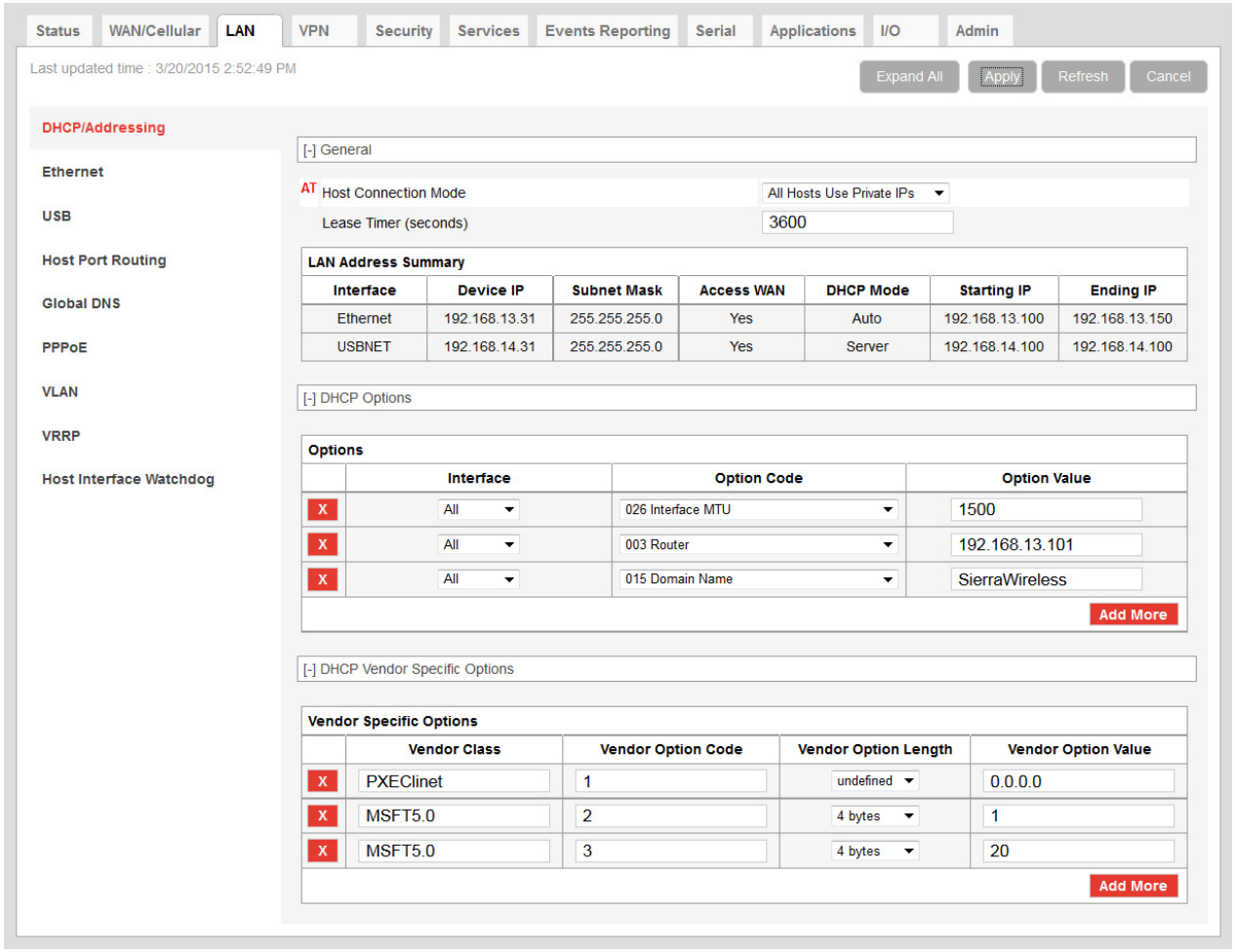


Figure 5-2: ACEmanager: LAN > DHCP/Addressing

Field	Description
General	
Host Connection Mode	Sets the Host Interface to use the Public IP address granted by the mobile network or private IP addresses. All host interfaces which are not using the public IP address use private IP addresses. The options are: • Ethernet Uses Public IP • All Hosts Use Private IPs—(default) • USB Uses Public IP* • Serial DUN Uses Public IP* • First Host gets Public IP* If you select this option, you do not have to specify the type of connection that uses the Public IP address. The first device to connect uses the Public IP address, regardless of whether it has a USB or Ethernet connection. * Until the gateway is able to obtain a mobile network connection, it provides private IP addresses in response to DHCP requests. For more information on Private and Public mode, see Private and Public Mode on page 79. *Note: If you plan on using Dynamic Mobile Network Routing (DMNR), select Ethernet Uses Public IP in this field.The connected computer receives the DHCP address from ALEOS and it also provides a static route (192.168.13.31 by default) that allows you to access ACEmanager from a connected device.*
Reset Host Interface	This field appears when Ethernet Uses Public IP or USB Uses Public IP is selected in the Host Connection Mode field. When this option is enabled, the host interface is reset when the device gets a new WAN IP. Options are: • Enable (default) • Disable
Public Mode Subnet Mask	This field appears when Ethernet, USB, or Serial (RS232) Uses Public IP is selected in the Host Connection Mode field. Public Mode subnet mask indicates the range of Public Mode host IP addresses. Options are: • 255.255.255.0 (24-bit) (default) • 255.255.255.255 (32-bit) Choose the option that matches the subnet mask received from the mobile network.
Lease Timer (seconds)	The amount of time the DHCP client is given for the use of the IP address (in seconds) Options are: • 120–4294967295—Number of seconds the IP address is leased for. If you want to set the value to “infinity”, enter 4294967295 (equivalent to 136 years). The actual maximum value depends on the maximum supported by your DHCP client. The default lease time is 3600 seconds (1 hour).
LAN Address Summary	Displays the interfaces which have been enabled. By default, only the Ethernet and USBNET Interfaces are enabled. This table also includes VLAN if configured.
Interface	The physical interface port or VLAN ID

Field	Description
Device IP	The IP address of the AirLink gateway for the specified interface port. By default, this is set to 192.168.13.31 for Ethernet, and 192.168.14.31 for USB/net.
Subnet Mask	Subnet mask indicates the range of host IP addresses that can be reached directly. Changing this limits or expands the number of clients that can connect to the AirLink gateway. The default of 255.255.255.0 means that 253clients can connect to the AirLink gateway. Uses 192.168.13. as the first three octets of the IP address if the gateway IP is 192.168.13.31.
Access WAN	Appears if the interface is configured to allow connected host(s) access to the Internet *Note: Internet access cannot be disabled for Ethernet hosts.*
DHCP Mode	Indicates whether or not the interface has a DHCP server enabled to provide dynamically allocated IP addresses provided to connected hosts *Note: The DHCP server can only be disabled for Ethernet and VLAN.*
Starting IP	Ethernet DHCP pool starting IP address (DHCP low address)
Ending IP	The ending IP for the interface (DHCP high address). If the starting and ending IP are the same, there is a single address in the pool and only one host receives an IP address from the DHCP server for that interface. Some interfaces, such as USB, can only have a single host connection. For others, statically assigned IP addresses in the same subnet, but outside of the DHCP pool, can still connect and use the gateway in the same way as a DHCP connected host.
Tip: *If you are using Private Mode for all hosts (*HOSTPRIVMODE=1), make sure that device IP, Starting IP, and Ending IP are on the same subnet defined by the DHCP network mask. If the subnet mask is 255.255.255.0, it is safe to use 192.168.x.y for each as long as the x is the same number (0 in the example screen shot above) and the y is different (1 and 2 in the example) and between 1 and 254.*	
DHCP Options Enables IT Administrators to configure up to 10 DHCP options, allowing you to push DHCP options to connected devices.	
Interface	Select the interface to use: • All (default) • Ethernet *Note: USB*VLAN *hosts only receive the DHCP options when the Interface is set to All.*
Option Code	Choose from the options in the drop-down menu. For a list of supported Option Codes, see Table 5-1. For additional information on the option codes, refer to the Internet Engineering Task Force (IETF) memorandum on Internet Protocols and Standards, RFC-2131.
Option Value	The format for the option value depends on the Option Code selected, as formats must conform with RFC 2132. For a list of accepted formats for each of the supported DHCP Option Codes, see Table 5-1. Use a comma to separate multiple values.

Field	Description
DHCP Vendor Specific Options Enables IT Administrators to configure up to 5 vendor-specific options	
Vendor Class	Enter the vendor class
Vendor Option Code	Enter the vendor option code. Possible entries are: • 0–255
Vendor Option Length	This field allows you to specify the DHCP vendor specific option length in order to ensure that the DHCP datagram is correctly formatted for the DHCP client. Options are: • Undefined—Use this setting for IP addresses and strings (default) • 1 byte—Use for decimal values of 255 or less • 2 bytes—Use for decimal values between 256 and 65535 • 4 bytes—Use for decimal values greater than 65535 *Note: If the size used for the data is not correct, the option is ignored by the client.*
Vendor Option Value	Enter the vendor option value in one of the following formats: • Dotted-quad IPv4 address • Decimal number • Colon-separated hex digits • Text string Use a comma to separate multiple values.

Table 5-1: Supported DHCP Options

DHCP Option	Type of entry	Accepted values (if applicable)
002 Time Offset	32-bit unsigned integer	-43200–43200[a]
003 Router	1 or more IP addresses	
007 Log Server	1 or more IP addresses	
009 LPR Server	1 or more IP addresses	
013 Boot File Size	16-bit unsigned integer	1–65535
015 Domain Name	Fully Qualified Domain Name (FQDN)	
016 Swap Server	1 or more IP addresses	
017 Root Path	ASCII string	
018 Extension Path	ASCII string	
019 IP Forward Enable/Disable	Single octet Boolean	0 (Disable) or 1 (Enable)
020 Non-Local Source Routing	Single octet Boolean	0 (Disable) or 1 (Enable)

Table 5-1: Supported DHCP Options

DHCP Option	Type of entry	Accepted values (if applicable)
021 Policy Filter	1 or more pairs of IP addresses or IP address/mask pairs	
022 Max Datagram Reassembly Size	16-bit unsigned integer	576–65535
023 IP TTL	8-bit unsigned integer	1–255
026 Interface MTU	16-bit unsigned integer	68–65535 (Default is 1500.)
027 All Subnets Are Local	Single octet Boolean	0 (Disable) or 1 (Enable)
031 Perform Router Discovery	Single octet Boolean	0 (Disable) or 1 (Enable)
032 Router Solicitation Address	Single IP address	
034 Trailer Encapsulation	Single octet Boolean	0 (Disable) or 1 (Enable)
035 ARP Timeout	32-bit unsigned integer	6–65535
036 Ethernet Encapsulation	Single octet Boolean	0 (Disable) or 1 (Enable)
037 TCP TTL	8-bit unsigned integer	1–255
038 TCP Keepalive	32-bit unsigned integer	0–65535
040 NIS Domain	ASCII string	Domain name
041 NIS Server	Single IP address	
042 NTP Server	Single IP address	
044 NetBIOS Name Server	1 or more IP addresses	
045 NetBIOS Datagram Distribution Server	1 or more IP addresses	
046 NetBIOS Node Type	8-bit unsigned integer	1, 2, 4, or 8
047 NetBIOS Scope	ASCII string	
048 X Windows System Font Server	1 or more IP addresses	
049 X Windows System Display Manager	1 or more IP addresses	
064 NIS+ Domain	Domain name	
065 NIS+ Server	Single IP address	
066 TFTP Server	ASCII string or IP address	Name, domain name, or IP address
067 Bootfile Name	ASCII string	Name
068 Mobile IP Home	1 or more IP addresses	
069 SMTP Server	1 or more IP addresses	
070 POP3 Server	1 or more IP addresses	

Table 5-1: Supported DHCP Options

DHCP Option	Type of entry	Accepted values (if applicable)
071 NNTP Server	1 or more IP addresses	
074 IRC Server	1 or more IP addresses	

a. The time offset is entered as seconds. See Table 5-2 for a list of hour/second conversions.

Table 5-2: Time Offset Hour/Second conversions

Hour	Seconds	Hour	Seconds
0	0		
1	3600	**-1**	-3600
2	7200	**-2**	-7200
3	10800	**-3**	-10800
4	14400	**-4**	-14400
5	18000	**-5**	-18000
6	21600	**-6**	-21600
7	25200	**-7**	-25200
8	28800	**-8**	-28800
9	32400	**-9**	-32400
10	36000	**-10**	-36000
11	39600	**-11**	-39600
12	43200	**-12**	-43200

Internal DHCP Server

DHCP (Dynamic Host Configuration Protocol) has become a primary component of today's network environments. DHCP allows one server to automatically and dynamically allocate network IP addresses and other network related settings (such as subnet masks, routers, etc.) to each computer or device without the need to set up each specifically or keep track of what addresses have already been used.

In a default configuration, the AirLink gateway acts as a DHCP host to any device connected to its ports. This DHCP host provides that device with an IP address that can be used to communicate on the Internet.

Address Assignment in Public Mode

1. When the AirLink gateway registers on the mobile network, it is assigned an IP address from the carrier, e.g., 10.1.2.0.

2. When using a specific interface, the AirLink gateway acts as a DHCP server unless disabled. When the Host Connection Mode is Ethernet Uses Public IP, and the AirLink gateway receives a DHCP request from an Ethernet device connected to its ports, it hands off the assigned address to the device and sets up the default gateway address as 10.1.2.1. If the fourth octet value is already a 1, it assigns 10.1.2.2 as the router address.

Note: The primary gateway to the mobile network, for any connected device, is enabled by default.

3. The AirLink gateway also sends a /24 netmask (255.255.255.0 by default) and sets up a static route which maps 192.168.13.31 (or the address configured with *HOSTPEERIP if it is changed) to 10.1.2.1 (or 10.1.2.2 if that was what the gateway address was given as).

Tip: *When PPPoE is used with the AirLink gateway, the DHCP server needs to be disabled. A tunnel is set up connecting a device (such as your computer or a router) with the AirLink gateway. The device then uses the MAC address of the AirLink gateway to send all outgoing packets.*

Ethernet

The AirLink gateway is equipped with an Ethernet port that can be enabled or disabled as needed. When the port is disabled, the host cannot connect via Ethernet, and ARP queries do not receive responses on the port.

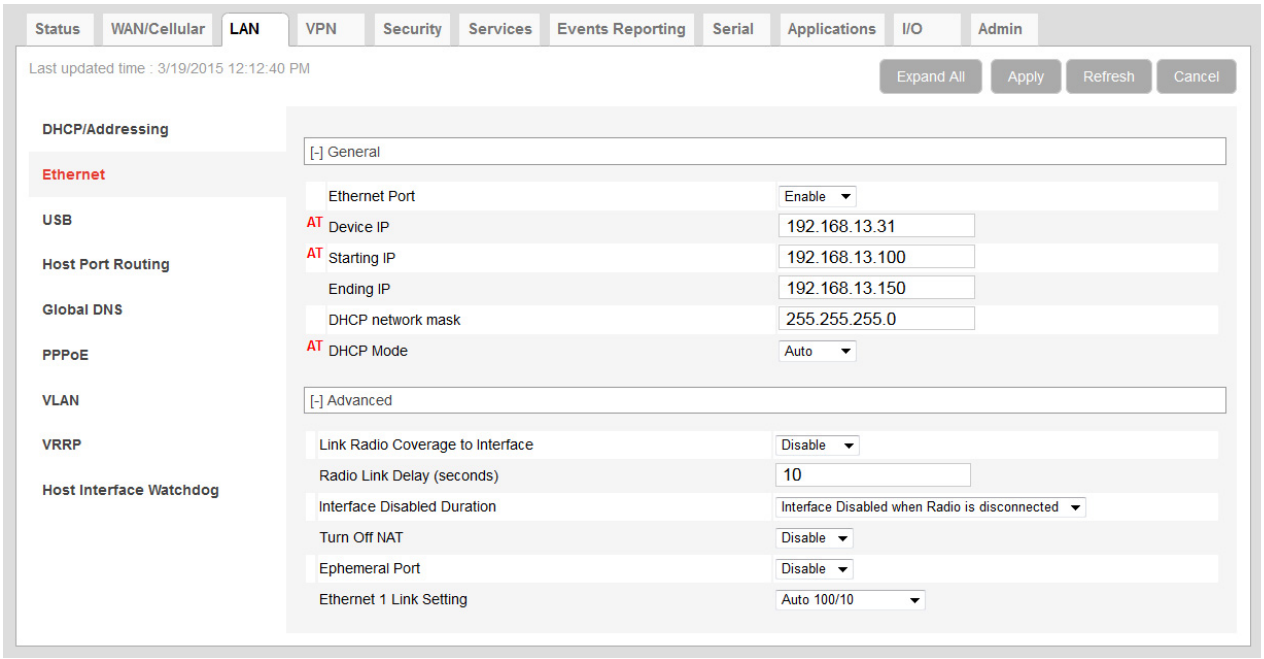


Figure 5-3: ACEmanager: LAN > Ethernet

Field	Description
General	
Ethernet Port	Enabled or Disabled *Note: When the port is disabled, the device ignores any physical connection to the Ethernet port.*
Device IP	The Ethernet IP address of the AirLink gateway. By default this is set to 192.168.13.31.
Starting IP	Ethernet DHCP pool starting IP address Default is 192.168.13.100. *Note: If only one computer or device is connected directly to the Ethernet port, this is the IP address it is assigned.*
Ending IP	The ending IP address for the Ethernet interface DHCP pool Default is 192.168.13.150.
DHCP network mask	The Netmask given to any Ethernet DHCP client Default is 255.255.255.0.
DHCP Mode	Determines how DHCP operates on the Ethernet interface Options are: • Server—The AirLink gateway acts as a DHCP server for all Ethernet connections. • Disable—The AirLink gateway acts as neither a DHCP server or client. All devices connected to the AirLink gateway must have a static LAN IP or use PPPoE. • Auto—When the gateway is powered on or reboots, it attempts to determine if a DHCP server is present on the Ethernet network. If a DHCP server is found, the gateway obtains an IP address and uses Ethernet for communication with AirLink Management Service (ALMS). If a DHCP server is not found, the gateway becomes a DHCP server. (default) Most of the time you can leave this field set to the default value.
Advanced	
Link Radio coverage to Interface	This disables the specified port when there is no cellular coverage. Options are: • Disable (default) • Ethernet • USB
Radio Link Delay (seconds)	The delay in seconds before the selected interface goes down when there is no cellular coverage

Field	Description
Interface Disabled Duration	Sets the period of time (in seconds) that the LAN interface is disabled when linking a LAN port to radio coverage. Either the Ethernet or the USB LAN port can be linked to the radio coverage, but not at the same time. Options are: • Interface Disabled when Radio is disconnected (default) • 5 Sec • 10 Sec • 15 Sec • 20 Sec • 25 Sec • 30 Sec
Turn Off NAT	When enabled, ALEOS routes outbound packets from connected devices without performing NAT on them. For example, when a connected device that has an IP address of 192.168.13.100 sends data to a remote destination, the outbound packets have a source IP of 192.168.13.100. In most cases, it is best to leave this field at the default setting (Disabled), as most mobile network operators do not support this functionality.
Ephemeral Port	Enable or Disable the Ephemeral Port feature • Disable—The source port in packets the AirLink gateway receives from a host device and then sends out is not changed. The source port assigned to the packet when it was created in the customer's host device is used. (default) • Enable—The AirLink gateway changes the source port on all outgoing NATed UDP packets, using the range configured in the Starting Ephemeral Port field.

Field	Description
Starting Ephemeral Port	This field appears only when the Ephemeral Port field is set to Enable. It allows you to set the starting port range used by a LAN host as the source port for over-the-air (OTA) destinations using NAT. *Note: This field is intended for advanced users only. In most cases, use the default value.* The NAT for the LAN host uses a range of 1000 ports as source ports for OTA destinations beginning with the configured Ephemeral port. Options are: • 1024 (default)–64535 If you have a network with multiple LAN hosts that are sending data to the same server and the server is not receiving data from one (or more) of the hosts, it may be because the Mobile Network Operator has a WAN firewall that is blocking the ports used by the NAT for over-the-air (OTA) destinations. This field enables you to avoid the blocked ports by changing the source port range used to send the data. For example, some users have found that changing the starting port to 42000 has resolved the issue. *Note: The ephemeral port setting does not affect any outbound traffic initiated by the device such as Events Reporting, Device Initiated AVMS connection, etc.*
Ethernet 1 Link Setting	Configures the Ethernet port speed and duplex setting Most of the time you can leave the default setting and the device you are connecting automatically negotiates the speed and duplex setting with the AirLink gateway. However, if the connected device has a fixed setting, use this field to change the AirLink gateway setting to match that of the connected device. The options are: • Auto 100/10 (default) • Auto 10 Mb only • 100 Mb Full Duplex • 100 Mb Half Duplex • 10 Mb Full Duplex • 10 Mb Half Duplex You can view the current speed and duplex setting on the Status > LAN page. See page 39.

USB

The AirLink gateway is equipped with a USB port that increases the methods by which you can send and receive data from a connected computer. You can set up the USB port to work as either a virtual Ethernet port or a virtual serial port, or you can disable it to prevent access by USB. You may need to install a USB driver to use these modes. For more information, see Installing the USB Drivers on page 92.

By default, the port is set to work as a virtual Ethernet port.

Note: Sierra Wireless recommends that you use a USB 2.0 cable with your AirLink gateway and connect directly to your computer for best throughput.

To change the USB port to allow virtual serial port communication:

1. In ACEmanager, go to LAN > USB, and choose USB Serial as the USB Device Mode.

To disable the USB port, select Disable from the same menu.

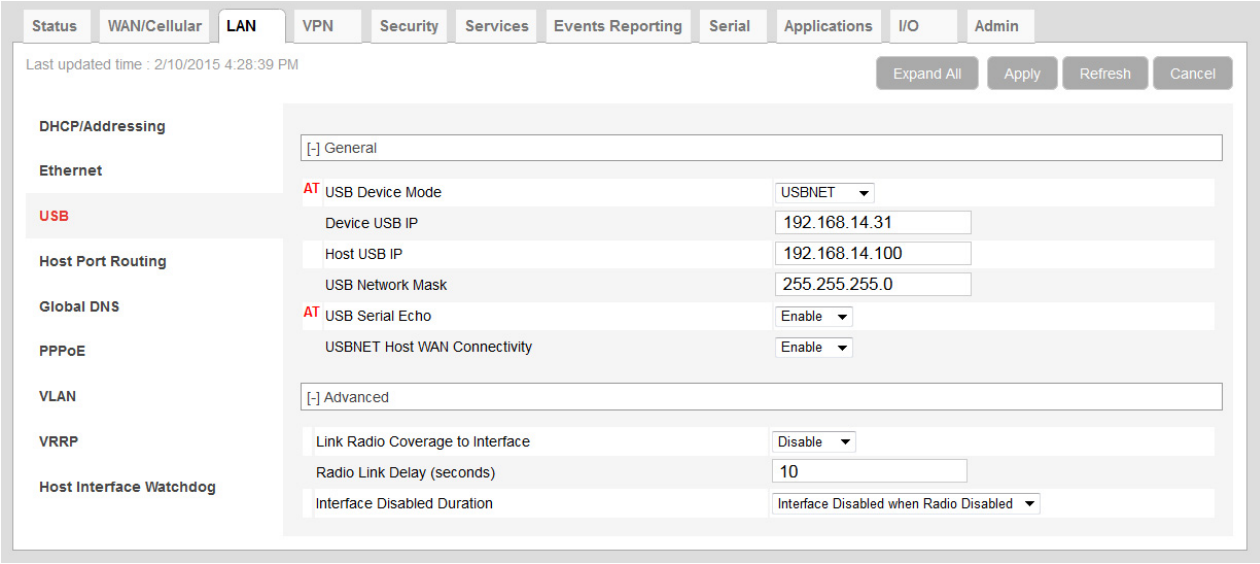


Figure 5-4: ACEmanager: LAN > USB

Field	Description
General	
USB Device Mode	The USB mode on gateway startup • USB Serial—USB port acts as a virtual Serial port. • USBNET—USB port acts as a virtual Ethernet port. (default) • Disabled—USB port is disabled. You can also configure this parameter using the AT Command *USBDEVICE. See *USBDEVICE on page 298. *Note: A reboot is required to activate the USB mode change.*
Device USB IP	The USBNET IP address of the AirLink gateway. By default this is set to 192.168.14.31.
Host USB IP	The IP for the computer or device connected to the USB port
USB Network Mask	Use this field to configure a subnet mask for USBNET Default is 255.255.255.0
USB Serial Echo	The AT command echo mode when the USB is configured as a virtual serial port Options: • Enable—Echoes commands to the computer (so you can see what you type) (default) • Disable—Does not echo commands to the computer (you cannot see what you type)

Field	Description
USBNET Host WAN Connectivity	Controls access to the WAN over the USB port Options are: • Enable—USB can be used to access the WAN (default) • Disable—Access to the WAN over USB is blocked.
Advanced	
Link Radio Coverage to Interface	Disables the specified port when there is no cellular coverage. Options are: • Disable (default) • Ethernet • USB
Radio Link Delay (seconds)	The delay in seconds before the selected interface goes down when there is no cellular coverage Valid range is 0–65535. Default is 10.
Interface Disabled Duration	Sets the period of time (in seconds) that the LAN interface is disabled when linking a LAN port to radio coverage. Either the Ethernet or the USB LAN port can be linked to the radio coverage, but not at the same time. Options are: • Interface Disabled when Radio Disabled (default) • 5 seconds • 10 seconds • 15 seconds • 20 seconds • 25 seconds • 30 seconds

Installing the USB Drivers

A USB driver is required if you want to use the USB port on the gateway as a virtual serial port (USB Serial). If you want to use the USB port as a virtual Ethernet port (USBnet), a driver is not required as the default Microsoft Windows 7 and Windows 8 drivers are used.

To install the USB Serial drivers for Windows 7 and Windows 8:

1. Go to source.sierrawireless.com and download the USB Serial Driver One-Click Tool.
2. Double-click the downloaded file (AirLink_Serial_<version number>.exe).
3. As the drivers installs, a progress box appears in the lower right-hand corner of the monitor.

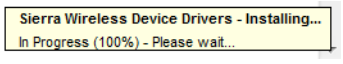


Figure 5-5: USB Serial One-Click Tool progress window

4. In ACEmanager, go to LAN > Ethernet and set the USB Device Mode field to USB Serial.
5. Connect a gateway to the computer using a USB cable.

   The driver installation completes and a window opens indicating the Serial Port number.

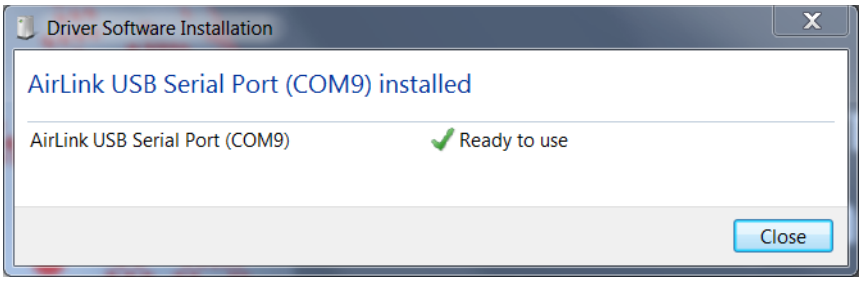


Figure 5-6: USB Serial Driver Installation Complete

At any time, you can open Device Manager to check the Serial Port number.

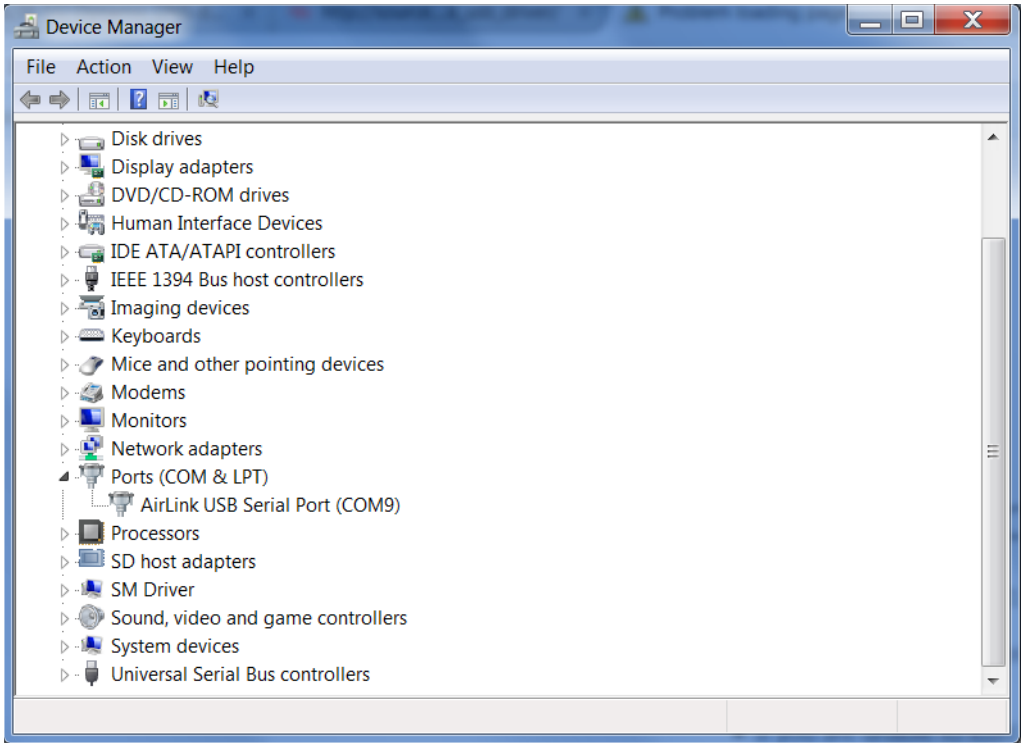


Figure 5-7: Device Manager

Note: USB serial and USBnet drivers available at source.sierrawireless.com also work with Linux CDC-ACM drivers.

Note: The COM port number assigned by driver installation is the next port that is available.The port number might vary depending on the number of devices connected (using serial or virtual serial).

Once the driver is installed, you can use the USB port just like a standard serial port.

Host Port Routing

Host port routing enables the AirLink gateway to handle network communication for up to two non-NATed networks behind the gateway or router connected to the AirLink gateway. The following illustration shows a typical network configuration. Figure 5-8 shows how ALEOS would be configured for the sample network shown.

Note: The AirLink gateway does not handle addressing for devices behind the router or gateway.

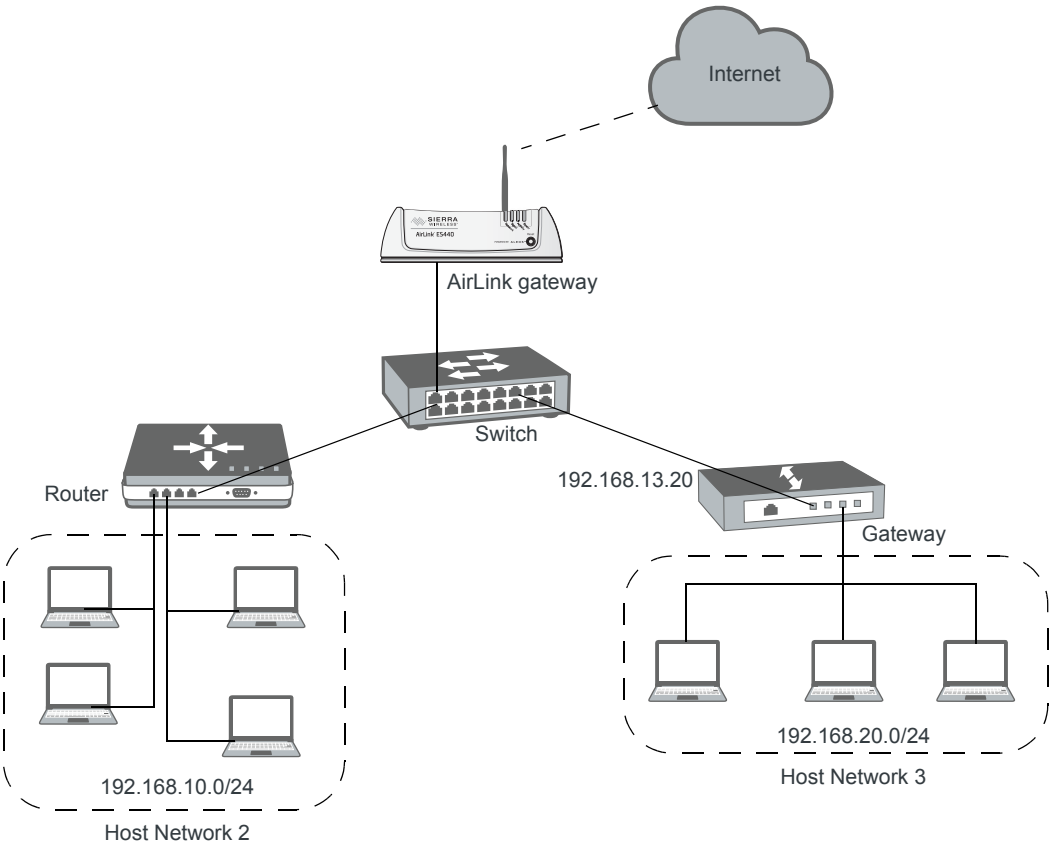


Figure 5-8: Host Port Routing Network Configuration

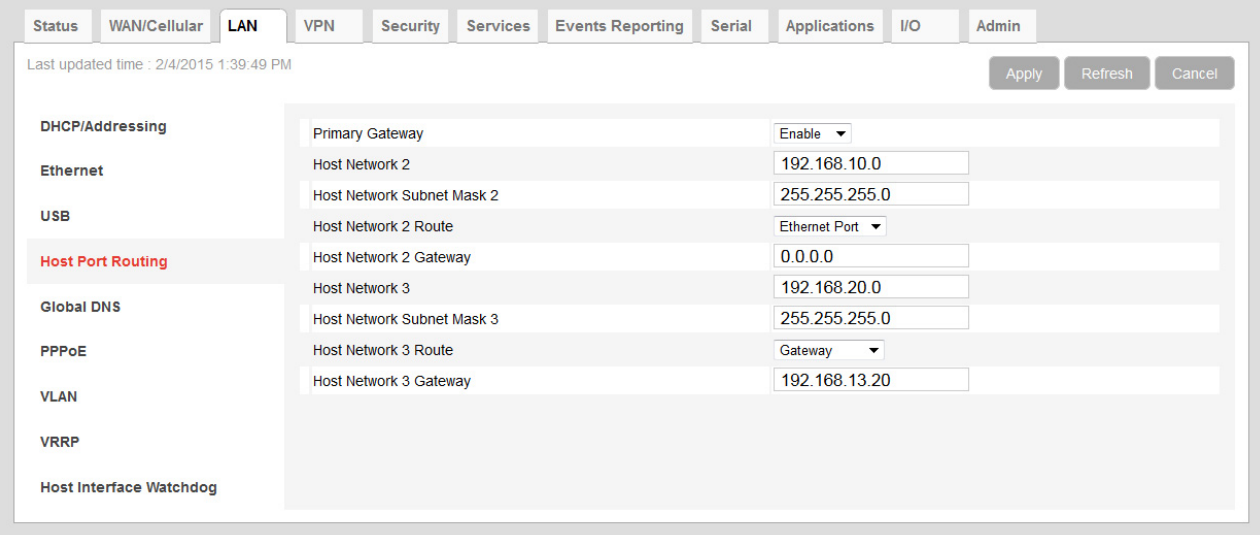


Figure 5-9: ACEmanager: LAN > Host Port Routing

Field	Description
Primary Gateway	When enabled, your AirLink gateway is the primary gateway for connected LANs and responds to Address Resolution Protocol (ARP) requests to resolve WAN addresses for devices on the connected LANs. Default is Enabled.
Host Network 2 and Host Network 3	Enter the IP address for Host Network 2 and 3. These are LAN networks connected to the AirLink gateway behind a router or gateway. They do not have the same IP range as the AirLink gateway LAN network. For example, 192.168.10.0.
Host Network Subnet Mask 2 and Host Network Subnet Mask 3	The subnet for the applicable network. For example, 255.255.255.0, which would with the setting above define a secondary network of 192.168.10.0/24.
Host Network 2 Route and Host Network 3 Route	Choose the appropriate option, depending on how ARP requests are handled on the network. Options are: • Ethernet — Select this option if the network uses a router that acts as an ARP proxy for addresses on subnets connected to it. For example, in Figure 5-8 on page 94, when traffic is destined for host 192.168.10.100 in network 2, the AirLink gateway sends an ARP request for 192.168.10.100. Note: If proxy ARP is not enabled on the router, the transmission fails (destination unreachable). • Gateway — Select this option if the network uses a device that does not handle ARP requests for network devices attached to it. When Gateway is selected, ALEOS handles ARP requests for the connected LAN devices. Any traffic destined for a host on the network behind a gateway is routed, by the device, through the gateway IP. For example, in Figure 5-8 on page 94, when traffic is destined for host 192.168.20.100 in network 3, the AirLink gateway sends an ARP request for the gateway (192.168.13.20), not the host. When you select Gateway, proxy ARP is not required on the router.
Host Network 2 Gateway and Host Network 3 Gateway	• If you selected Gateway in the Host Network Route field, enter the IP address for the gateway. • If you selected Ethernet in the Host Network Route field, leave this field as 0.0.0.0.

Global DNS

When the mobile network grants the IP address to the device, it includes the IP addresses of its DNS servers. Global DNS allows you to override the Mobile Network Operator's DNS settings for all connected devices. This is useful when the connected devices need to use a private network.

Note: If there are no alternate DNS servers defined, the default is the WAN network DNS server.

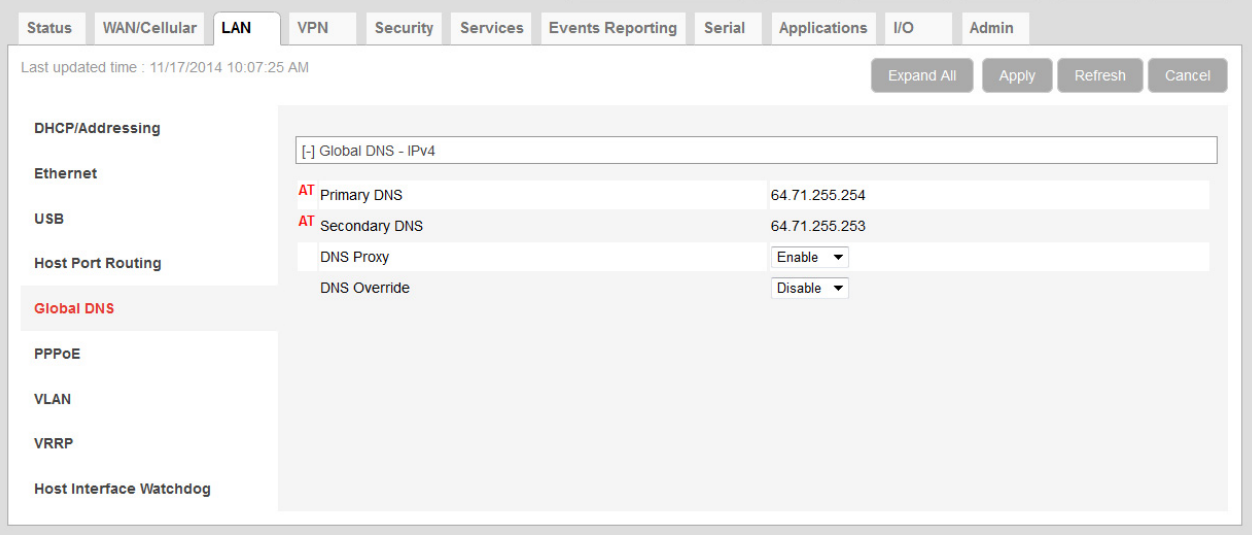


Figure 5-10: ACEmanager: LAN > Global DNS

Field	Description
Primary DNS	Primary Mobile Network Operator's DNS IP Address. This and the secondary DNS are generally granted by the mobile network along with the Network IP.
Secondary DNS	Secondary Mobile Network Operator's DNS IP Address

Field	Description

DNS Proxy	Determines whether or not the AirLink gateway is used as a DNS proxy server.
	Note: Using the AirLink gateway as a proxy DNS server can help reduce mobile network data use.
	Options are:
	• Enable (default) —All connected DHCP clients (PPP, PPPoE, USBNET, and Ethernet) send their DNS IP address resolution requests to the AirLink gateway. The AirLink gateway performs DNS lookups on behalf of the DHCP client.
	  • If the AirLink gateway is able to resolve the request, it sends a response to the DHCP client.
	  • If the AirLink gateway does not have the necessary information to resolve the request, it sends the request to the DNS server configured in the DNS Override field. When the AirLink gateway receives a response, it forwards it to the DHCP client and saves the information so that it can resolve the same request in the future.
	• Disable—All connected DHCP clients send their DNS IP address resolution requests to the DNS server received from the mobile network or the alternate server specified by DNS Override, if enabled. The AirLink gateway is not used as a DNS server.

DNS Override	Overrides the Mobile Network Operator's DNS address with the DNS server configured in the Alternate Primary DNS and Alternate Secondary DNS fields. Options are: • Disable (default)—Mobile Network Operator's DNS server is used • Enable—Alternate DNS server is used
Alternate Primary DNS	Configure the primary DNS server to use instead of the Mobile Network Operator's DNS server
Alternate Secondary DNS	Configure the secondary DNS server to use instead of the Mobile Network Operator's DNS server
Alternate DNS Port	If you want to specify the port on the connected device that the AirLink gateway sends IP address resolution responses to: 1. Ensure that the DNS Override field is set to Enable. 2. Enter the desired port number in this field. 3. Click Apply. When this field is set to 53 (default) or 0, packets are sent to port 53, the standard DNS port.

PPPOE

PPPoE (Point-to-Point Protocol over Ethernet) allows a point-to-point connection while using Ethernet. Just like the dial up protocol on which it is based, PPPoE can use traditional user name and password authentication to establish a direct connection between two Ethernet devices on a network (e.g., your AirLink gateway and your computer or router).

examples for PPPoE with your AirLink gateway:

- Backup connectivity solution for your network
- Individualized Internet connection on a LAN

- Password restricted Internet connection

Only one computer, router, or other network device at a time can connect to the AirLink gateway using PPPoE. If you are using the AirLink gateway connected to a router as a back up Internet connection for your network, you should configure the router to use the PPPoE connection and not the individual computers.

Note: To configure a PPPoE connection on some operating systems, you need administrator privileges to the computer you are configuring or access granted by an administrator on the network to add/remove devices to your computer.

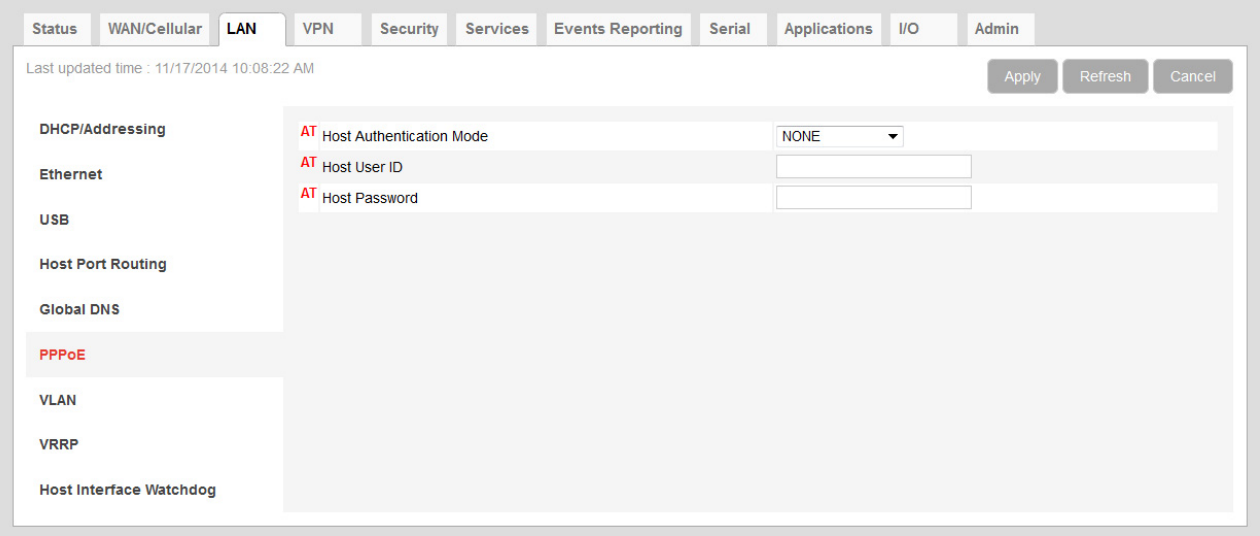


Figure 5-11: ACEmanager: LAN > PPPoE

Field	Description
Host Authentication Mode	Host Authentication Mode: Use PAP or CHAP to request the user login and password during PPP or CHAP negotiation on the host connection. The username and password set in *HOSTUID and *HOSTPW is used. • NONE (default) • PAP and CHAP • CHAP
Host User ID	User ID for authentication (up to 64 bytes)
Host Password	Password for authentication

Configure the AirLink gateway to Support PPPoE

Note: You must disable the DHCP server for PPPoE to work.

To configure an AirLink gateway to support PPPoE:

1. In ACEmanager, go to LAN > Ethernet.
2. Under General, in the DHCP Server Mode field, select Disable.

Note: PPPoE authentication is optional. If you use PPPoE authentication, no other tethered LAN connection will have network access, regardless of whether or not the PPPoE host is connected. If you are using non-authenticated PPPoE, other tethered LAN connections will have network access until a PPPoE host is connected.

3. If you want to use authenticated PPPoE:
   a. Go to LAN > PPPoE, and in the Host Authentication Mode field, select PAP and CHAP.
   b. In the Host User ID, enter a user ID for the PPPoE connection.
   c. In the Host Password field, enter a password for the PPPoE connection.
4. Click Apply.
5. Reboot the gateway.

Tip: *If you leave Host User ID and Host Password blank, any computer or device can connect to the AirLink gateway using PPPoE.*

Note: ACEmanager shows the existing value for the PPPoE password as stars (****).

Optional: Configure the Device Name

1. In ACEmanager, go to Services > Dynamic DNS.
2. In the Service field, select IP Manager.
3. Under Dynamic IP, enter a name in the Device Name field, such as AirLink gateway or the ESN. The name can be up to 20 characters long.

   The name you choose for Device Name does not affect the connection, but may need to be configured in PPPoE settings for the router, device, or computer you connect to your AirLink gateway.

Configuring a PPPoE Connection in Windows 7

1. In Windows 7, go to Start > Control Panel.

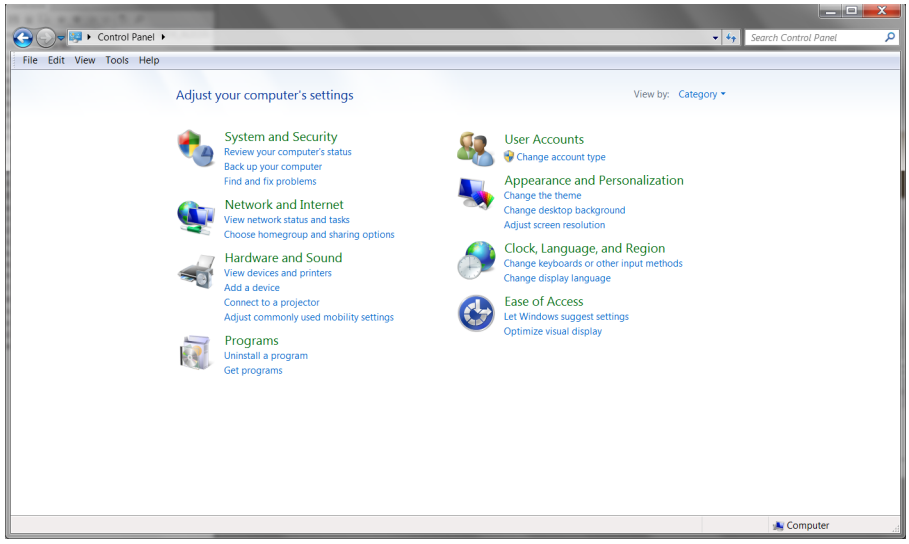


Figure 5-12: Windows 7: Control Panel

2. Select Network and Internet.

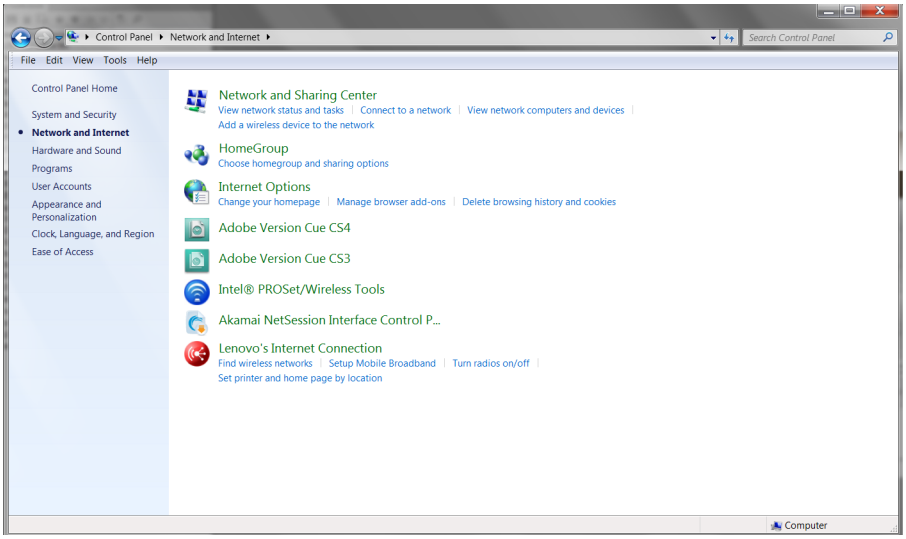


Figure 5-13: Windows 7: Control Panel > Network and Internet

3. Select Network and Sharing Center.

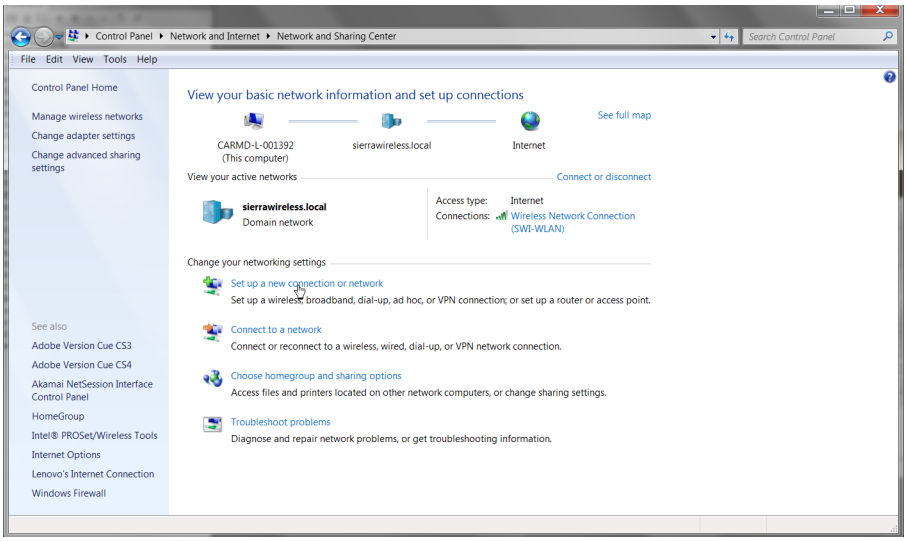


Figure 5-14: Windows 7: Control Panel > Network and Sharing Center

4. In the middle of the page, under Change your networking settlings, select Set up a new connection or network.

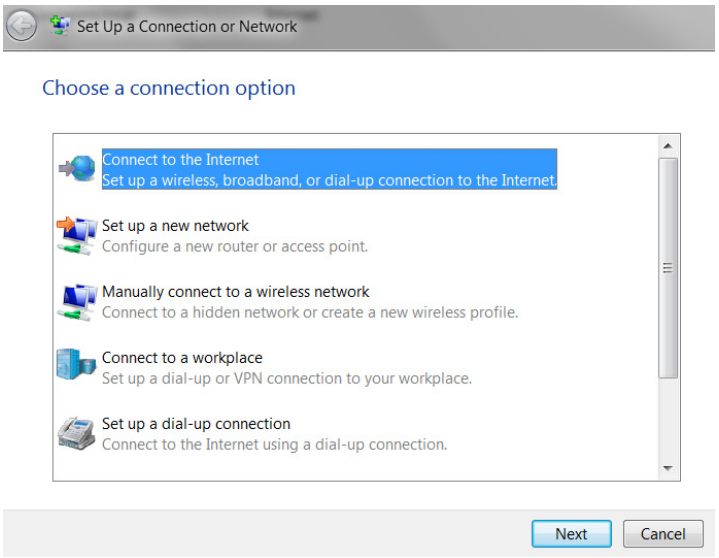
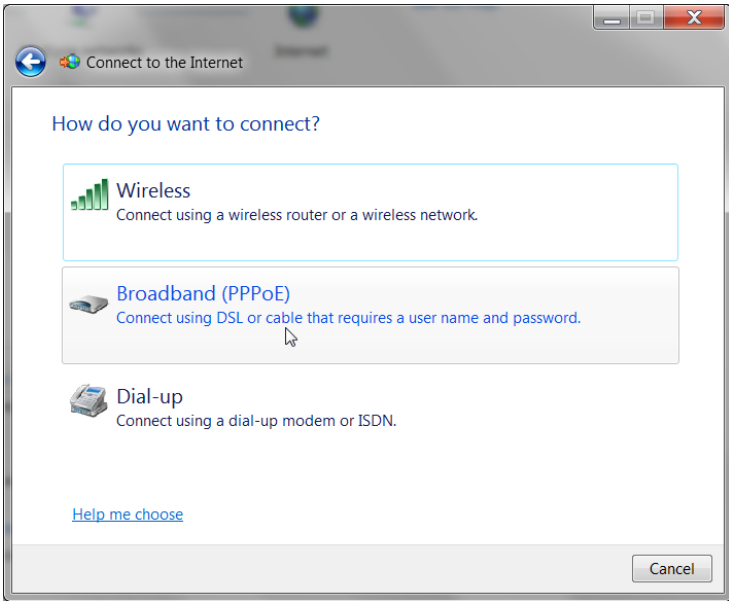
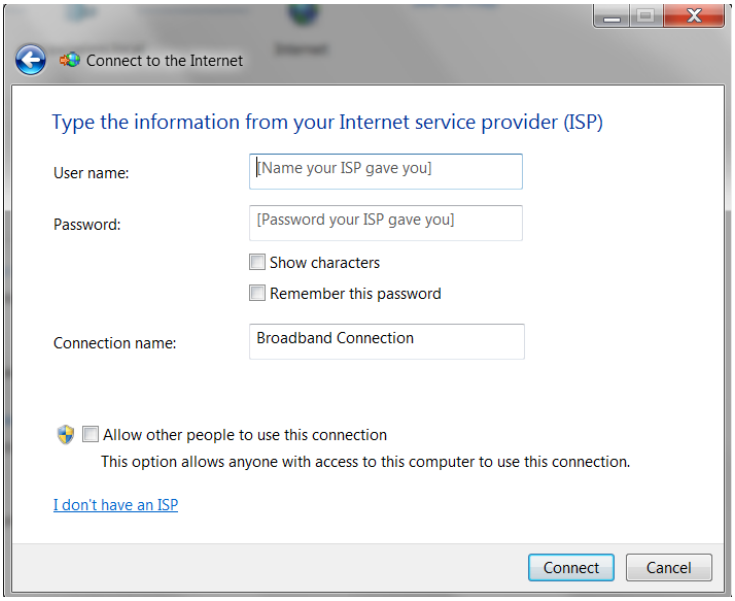


Figure 5-15: Set Up an Connection or Network

5. Select Connect to the Internet and click Next.



6. Select Broadband (PPPoE).



7. If you are using authenticated PPPoE, enter the User name and Password you configured in ACEmanager.
8. If desired, change the Connection name to something such as PPPoE that clearly identifies the connection.
9. Click Connect.

For subsequent connections, you can click the network icon in the Task bar ( ) and select the PPPoE connection.

VLAN

ALEOS supports up to three Virtual Local Area Networks (VLANs) on its Ethernet port. VLANs are logical groupings of network devices that share the same broadcast domain. All devices on the same VLAN can ping each other without routing. ALEOS does not support routing between VLANs.

Note: The VLANs must also be configured on the switch.

Figure 5-16 shows a network configured for two VLANs.

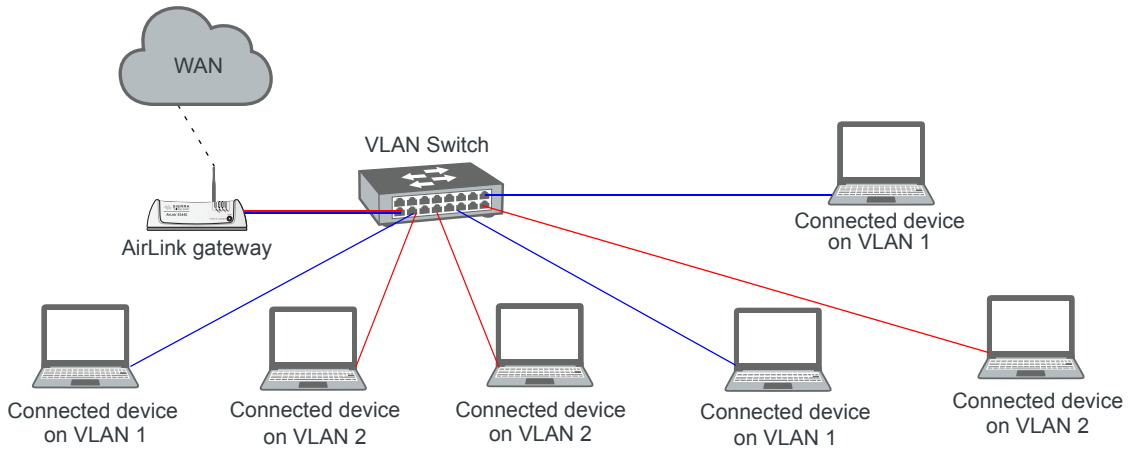


Figure 5-16: VLAN network configuration

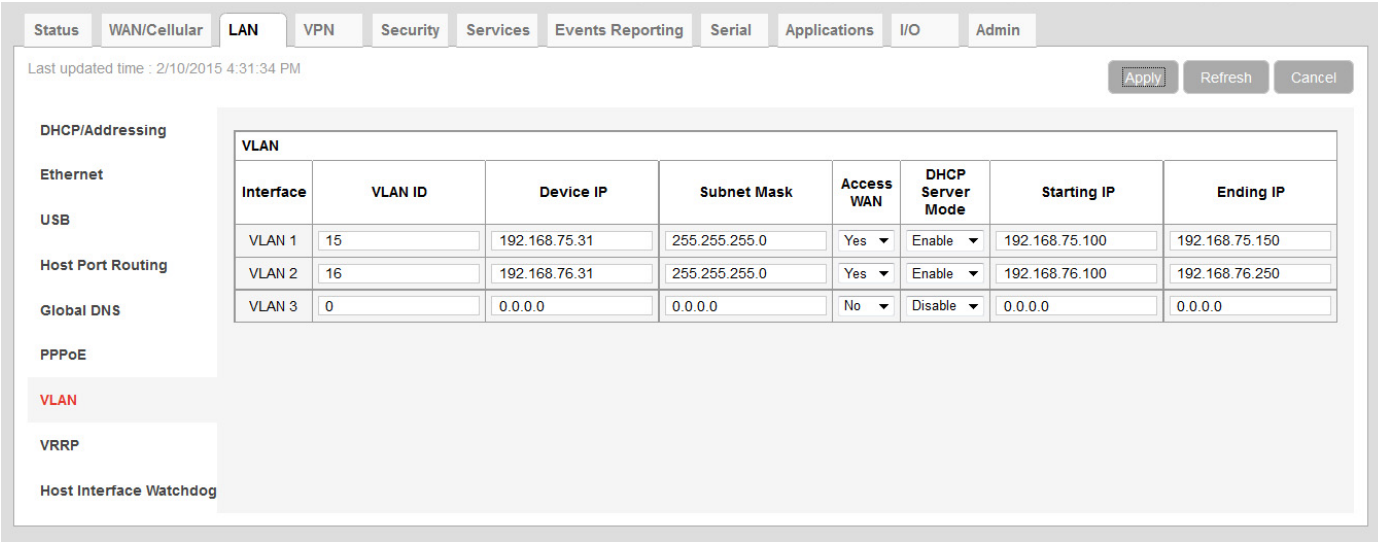


Figure 5-17: ACEmanager: LAN > VLAN

Field	Description
Interface	Displays the three VLANs you can configure
VLAN ID	VLAN ID • 0—VLAN is disabled (default) • 1–4094—Valid range for VLAN ID
Device IP	The IP address of the AirLink gateway for that VLAN interface
Subnet Mask	The subnet mask indicates the range of host IP addresses that can be reached directly. Changing the subnet mask limits or expands the number of devices that can connect to the AirLink gateway.
Access WAN	Choose whether or not devices on the configured VLAN have access to the WAN. • Yes • No
DHCP Server Mode	Choose whether or not the AirLink gateway acts as a DHCP server Options are: • Enable—AirLink gateway acts as the DHCP server • Disable (default)
Starting IP	VLAN interface DHCP pool starting IP address
Ending IP	VLAN interface DHCP pool ending IP address

VRRP

VRRP (Virtual Router Redundancy Protocol) enables you to configure a backup WAN connection to be used if the primary connection fails. You can configure VRRP on the AirLink gateway's Ethernet port or for VLANs.

You configure a VRRP Master and VRRP Backup device(s) and set their priorities. The device with the highest priority (normally the VRRP Master) becomes the primary route for the data connection.

The VRRP Master and Backups share a common virtual IP.

For information on configuring VLANs, see VLAN on page 103.

One common scenario is to use a 3rd party router for the primary connection and the AirLink gateway, either with or without VLANs, for the backup connection, as shown in Figure 5-18 and Figure 5-19.

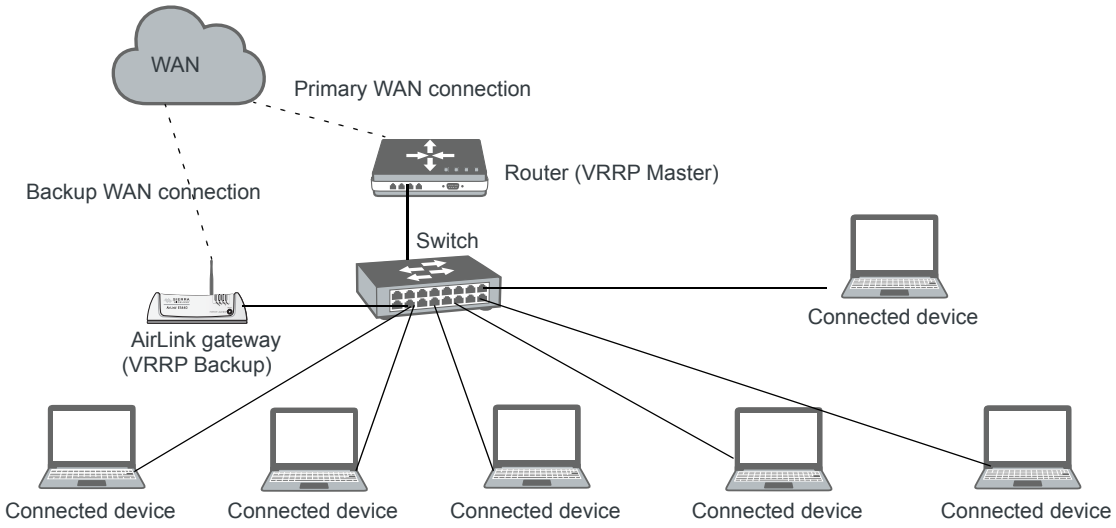


Figure 5-18: VRRP Network Configuration without VLANs

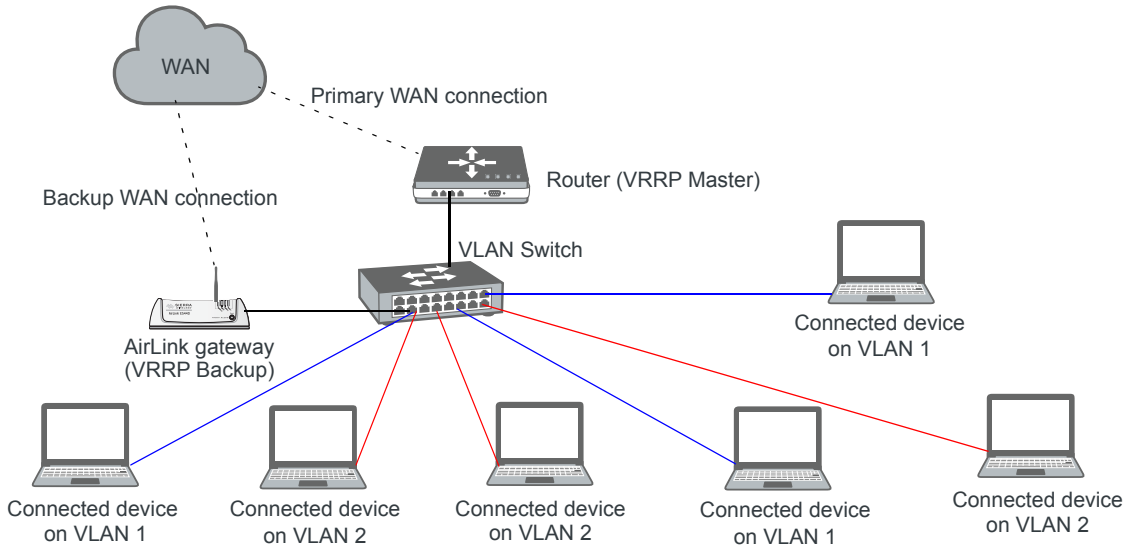


Figure 5-19: VRRP Network Configuration with VLANs

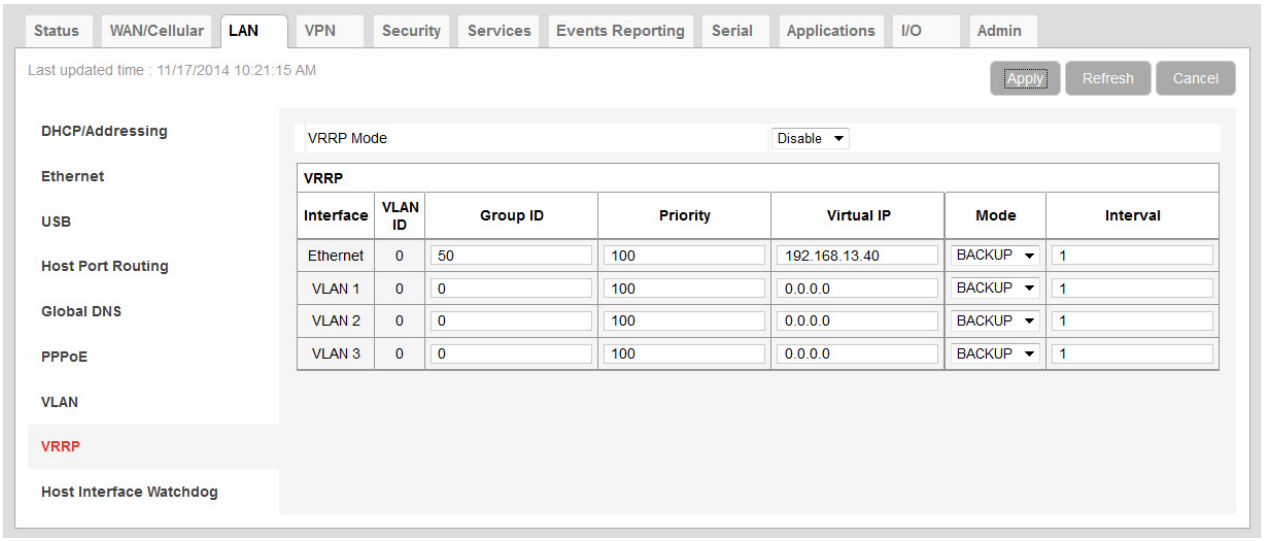


Figure 5-20: ACEmanager: LAN > VRRP (no VLANs)

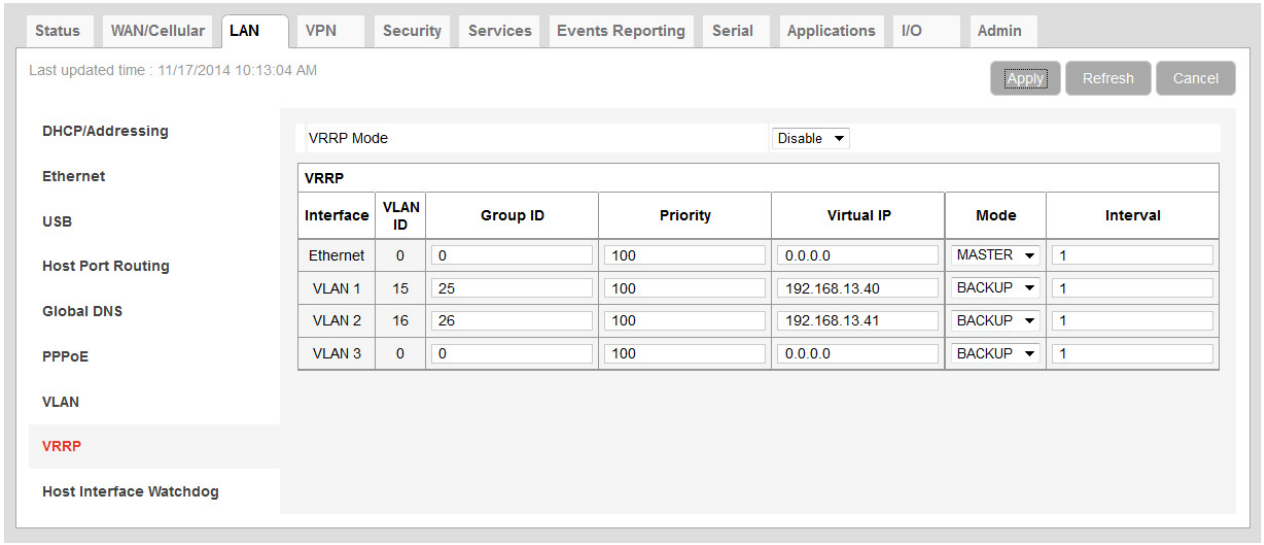


Figure 5-21: ACEmanager: LAN > VRRP (VLANs)

You can also set up VRRP using two AirLink gateways—one configured as the VRRP Master and the other as the VRRP Backup. The Backup AirLink gateway provides an alternate route when the Master AirLink gateway loses coverage.

For example, if you have cellular accounts with two different Mobile Network Operators (MNOs) you might prefer to use MNO A's connection, but to maintain continuity, you would like traffic to switch to MNO B if A's network is down and switch back to A's network once the connection is re-established, as shown in Figure 5-22.

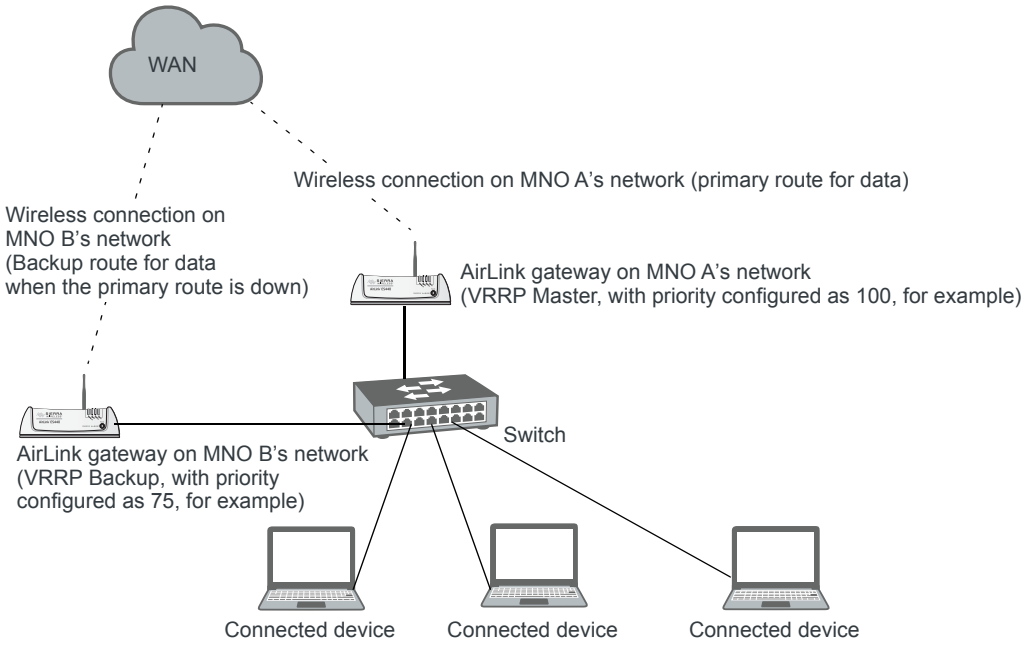


Figure 5-22: VRRP Network Configuration using two AirLink gateways

Field	Description
VRRP Mode	Allows you to activate VRRP. Options are: • Enable • Disable (default)
VRRP—The VLAN ID, Group ID, and Virtual IP address must be the same on the VRRP Master and VRRP Backup devices.	
Interface	Displays Ethernet port on AirLink gateway and the VLAN numbers
VLAN ID	Displays the VLAN ID This value is inherited from the LAN > VLAN screen. (See VLAN on page 103.) • 0—VLAN is disabled • 1–4094—Valid range for VLAN ID
Group ID	Enter the VRRP Group ID. Configure the VRRP Master (for example, the 3rd party router) and the VRRP Backup (for example the AirLink gateway) with the same Group ID. Options are: • 0–255 (Default is 0.)

Field	Description
Priority	Use this field to configure the priority for the AirLink gateway. The device with the highest priority (typically a 3rd party router) provides the primary data traffic route. If the device loses its connection to the WAN, its priority number drops. If the device fails, then when the failure is detected, the next highest priority router becomes the active router. The priority number configured on the VRRP Backup (typically the AirLink gateway) should be less than the initial priority number on the VRRP Master and greater than the value that the VRRP Master's priority number would be if it drops as a result of losing its WAN connection. For example, if the VRRP Master router has an initial priority number of 200 that drops to 80 if it loses its WAN connection, setting the AirLink gateway's priority to 100 ensures that it becomes the primary route if the VRRP Master loses its WAN connection. When the 3rd party router re-establishes its connection, its priority returns to 200 and it once again becomes the primary route for data. Options are: • 1–255 (Default is 100.)
Virtual IP	Configure the same virtual IP for the VRRP Backup (typically the AirLink gateway) and the VRRP Master (typically a 3rd party router). The virtual IP must be unique within the VLAN subnet and cannot be within a pool of addresses assigned via DHCP.
Mode	Indicates the initial mode for the AirLink gateway Options are: • MASTER • BACKUP (default) *Note: Designating a device as "Master" in this field does not make it the primary route for data unless it is also given a higher priority number than the VRRP Backup device. See Priority.*
Interval	If the AirLink gateway is acting as VRRP Master, it advertises its Master status at the interval (in seconds) configured in this field. Options are: • 1–65535 seconds (Default value is 1.)

Host Interface Watchdog

The Host Interface Watchdog provides a way for you to ensure that the LAN connection is alive. You can use this feature to monitor:

- A host connected to the LAN via an Ethernet or USB connection

When the Host Interface Watchdog is enabled, ALEOS sends a ping to the connected host at configured intervals. You can disable Force Keepalive to only send a ping when there is no traffic on the LAN interface. (See Force LAN Keepalive on page 109.)

If there is no response to the ping, the LAN interface is reset.

Note: The network interface is automatically determined from the IP address and the LAN configuration.

After the interface comes back up, ALEOS sends another ping to the connected host. If there is still no response to this ping, the AirLink gateway reboots. After a reboot caused by the LAN Interface Watchdog, ALEOS waits an hour before attempting pings to prevent repeated frequent reboots.

Note: DUN (PPP) is not supported. If the IP address for the host is on a DUN network, the feature is disabled.

Note: The feature is not disabled when the interface uses Public Mode, but it cannot monitor the host interface unless the mobile network provides a static IP.

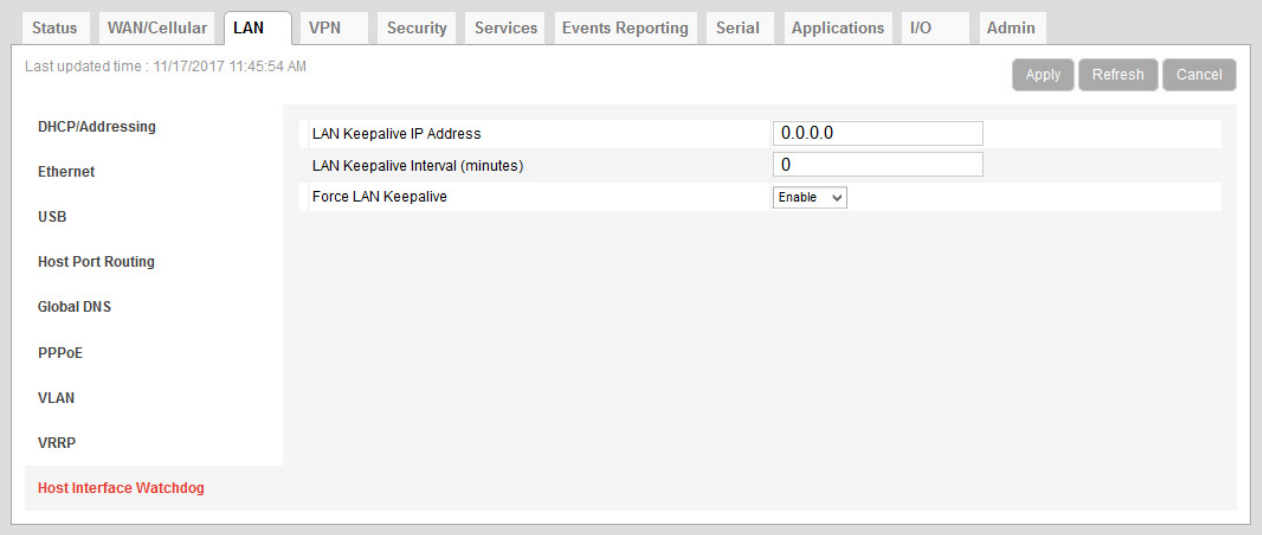


Figure 5-23: ACEmanager: LAN > Host Interface Watchdog

Field	Description
LAN Keepalive IP Address	Enter the IP address of the host to ping If a host IP address is not configured, the Host Interface Watchdog is disabled.
LAN Keepalive Interval (minutes)	The interval (in minutes) at which ALEOS pings the LAN-connected device Options are: 1–1440 If this field is set to 0, the Host Interface Watchdog is disabled. (default) To prevent the gateway from rebooting frequently when a connection is not available, if the gateway reboots as a result of a failed keepalive ping, it waits 60 minutes before sending another keepalive ping. Once the ping is successful, the gateway returns to the interval configured in this field.
Force LAN Keepalive	• Enable (default)—The network interface statistics are not monitored and a ping is always sent at the interval configured in the Keepalive Interval field. • Disable—The network interface statistics are monitored and connectivity is assumed when there is traffic received. A ping is only sent when there is no traffic for a period greater than the interval set in the Keepalive Interval field.

6: VPN Configuration

The AirLink gateway can act as a Virtual Private Network (VPN) device, providing enterprise VPN access to any device connected to the AirLink gateway even when a device has no VPN client capability on its own. The AirLink gateway supports three types of VPN: IPsec, GRE, and SSL. The AirLink gateway can support up to five VPN tunnels at the same time.

Note: Dynamic Mobile Network Routing (DMNR) is not compatible with VPN tunnels. If you are using DMNR, disable all VPN tunnels.

Split Tunnel

The AirLink gateway supports Global settings with one encrypted tunnel and one open tunnel. A sample server subnet for a Global setting would be 172.16.1.0/24. Global settings VPNs should be set up with care, as a Global settings configuration with both an enterprise VPN and access to the public Internet can inadvertently expose company resources.

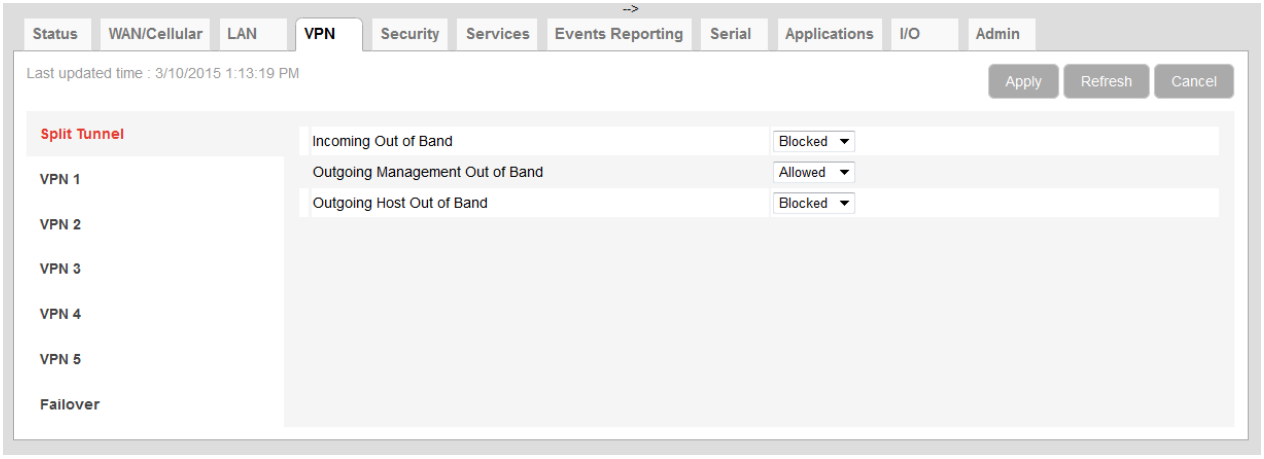


Figure 6-1: ACEmanager: VPN > Split Tunnel

Field	Description
Incoming Out of Band	Controls incoming public Internet traffic Options are: • Blocked—Incoming public Internet traffic is blocked. Only traffic through the VPN tunnel is allowed. (default) • Allowed—Incoming public Internet traffic is allowed.
Outgoing Management Out of Band	Controls outgoing traffic from the AirLink gateway • Blocked—Outgoing traffic from the AirLink gateway to the public Internet is blocked. Only traffic through the VPN tunnel is allowed. • Allowed—Outgoing traffic from the AirLink gateway to the public Internet is allowed. (default)
Outgoing Host Out of Band	Controls of outgoing Host out of band traffic. Options are: • Blocked—Public Internet traffic from the host device is blocked. Only traffic through the VPN tunnel is allowed. (default) • Allowed—Public Internet traffic from the host device is allowed.

IPsec Tunnel

The IP protocol that drives the Internet is inherently insecure. Internet Protocol Security (IPsec), which is a standards-based protocol, secures communications of IP packets over public networks.

IPsec is a common network layer security control and is used to create a virtual private network (VPN).

The advantages of using the IPsec feature includes:

- Data Protection: Data Content Confidentiality allows you to protect your data from any unauthorized view, because the data is encrypted (encryption algorithms are used).
- Access Control: Access Control implies a security service that prevents unauthorized use of a Security Gateway, a network behind a gateway or bandwidth on that network.
- Data Origin Authentication: Data Origin Authentication verifies the actual sender, thus eliminating the possibility of forging the actual sender's identification by a third-party.
- Data Integrity: Data Integrity Authentication allows both ends of the communication channel to confirm that the original data sent has been received as transmitted, without being tampered with in transit. This is achieved by using authentication algorithms and their outputs.

The IPsec architecture model includes the Sierra Wireless AirLink gateway as a remote gateway at one end, communicating through a VPN tunnel with a VPN gateway at the other end. The remote gateway is connected to a remote network and the VPN is connected to the local network. You can configure up to three remote subnets.

The IPsec VPN employs the IKE (Internet Key Exchange) protocol to set up a Security Association (SA) between the AirLink gateway and a Cisco (or Cisco compatible) enterprise VPN server. IPsec has two phases for setting up an SA between peer VPNs.

Phase 1 creates a secure channel between the AirLink gateway VPN and the enterprise VPN, thereby enabling IKE exchanges. Phase 2 sets up the IPsec SA that is used to securely transmit enterprise data.

Note: If you configure custom settings, they are saved and the tunnel can be disabled and re-enabled without needing to re-enter the settings. For a successful configuration, all settings for the VPN tunnel must be identical between the AirLink gateway VPN and the enterprise VPN server.

You can also configure VPN Failover for IPsec VPN tunnels. For more information, see VPN Failover on page 123.

To configure an IPsec VPN tunnel:

1. In ACEmanager, go to VPN.
2. Select the VPN you want to configure (1, 2, 3, 4, or 5).
3. In the VPN Type field, select IPsec Tunnel. The screen expands to show the IPsec Tunnel fields.

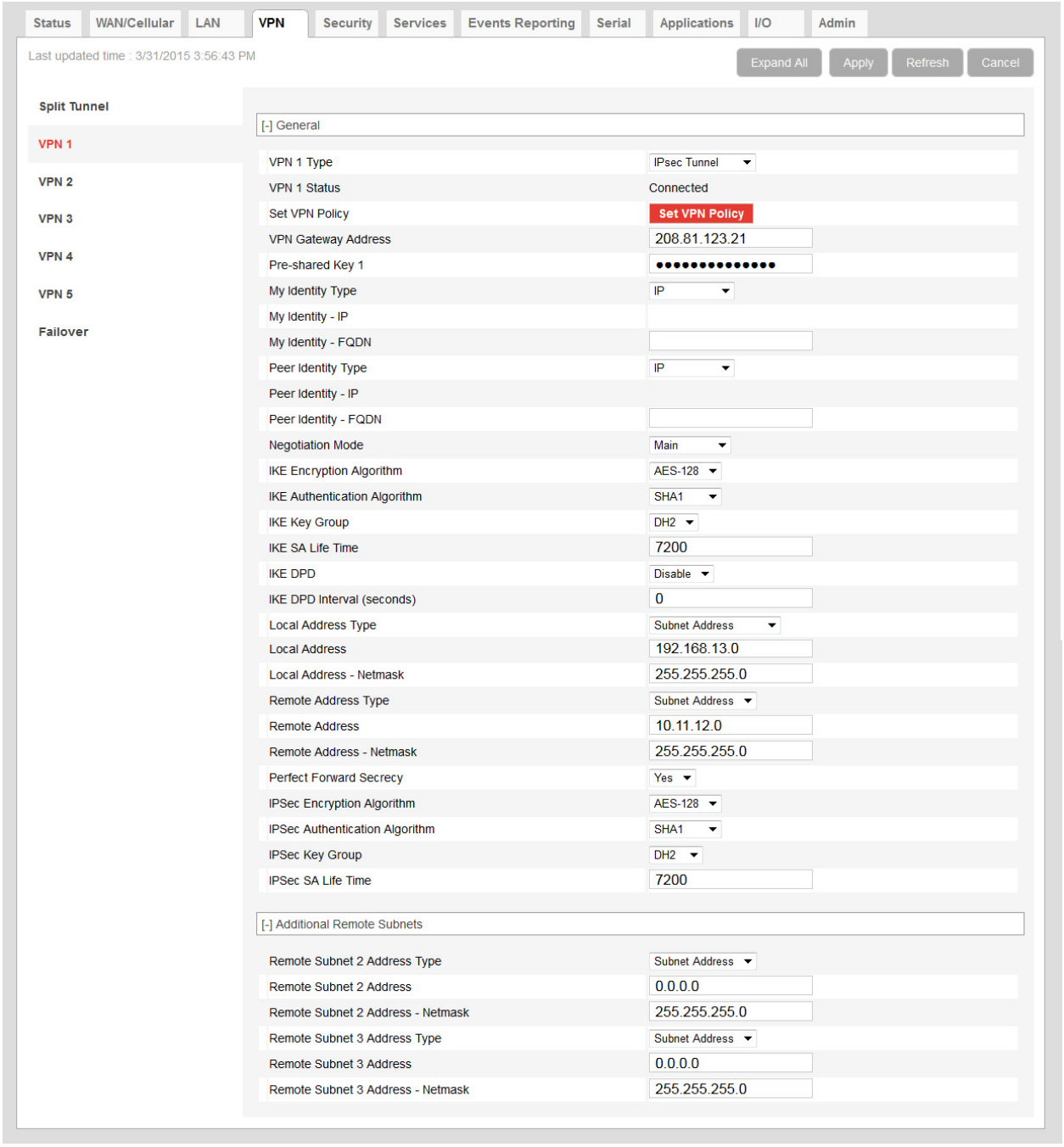


Figure 6-2: ACEmanager: VPN > VPN 1 > IPsec Tunnel

4. See the following table for instructions on completing the IPsec Tunnel fields.
5. Once the configuration is complete:
   a. Click the Set VPN Policy button.
   b. Check the VPN Status field to confirm the status of the VPN connection.

Field	Description
General	
VPN # Type	Use this field to select the type of VPN tunnel. If you configure custom settings, they are saved and the tunnel can be disabled and re-enabled without needing to re-enter the settings. Options are: • Tunnel Disabled (default) • IPsec Tunnel • GRE Tunnel • SSL Tunnel (only available for VPN 1)

VPN # Status	Status of the VPN connection:
	• Disabled—VPN is disabled (default)
	• Not Connected—The VPN failed to connect. This could be because of a mismatch in the configuration between the client and the server, no data connection on the device, etc.
	• Connected—The VPN is connected and ready to transmit traffic.
	• Configuration Error—This status appears when:
	  • Two VPNs have the same Local Address and Remote Address
	  • More than one VPN has the remote address set to “0.0.0.0”
	When either of these errors exist, only the first of the conflicting VPNs is operational.
	To determine which VPNs are in conflict:
	1. Go to Admin > Configure Log.
	2. For the VPN Subsystem, ensure that Display in Log is set to Yes. The Verbosity can be either Info or Debug.
	3. Click View Log.
	4. The resulting log shows you which VPNs are in conflict.

Set VPN Policy	After completing the VPN Configuration: 1. Click this button to apply the new settings. 2. Check the VPN Status field to confirm the status of the VPN connection. (See VPN # Status.)

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>VPN Gateway Address</td><td>The IP address of the server that this VPN client connects to. This address must be open to connections from the AirLink gateway. The default VPN Gateway IP Addresses are static address on Sierra Wireless Servers. They are:

<table>
<tr><th>VPN</th><th>Gateway IP Address</th></tr>
<tr><td>1</td><td>208.81.123.21</td></tr>
<tr><td>2</td><td>208.81.123.22</td></tr>
<tr><td>3</td><td>208.81.123.26</td></tr>
<tr><td>4</td><td>208.81.123.23</td></tr>
<tr><td>5</td><td>208.81.123.24</td></tr>
</table>

You can use these default IP addresses to confirm that an IPsec connection can be established with your wireless configuration before making any configuration changes, and as an example to model your VPN configuration after. (See Figure 6-4.)</td></tr>
<tr><td>Pre-shared Key 1</td><td>The pre-shared key (PSK) is used to initiate the VPN tunnel.
• Pre-shared key length: Maximum supported length is 128 characters.
• Valid characters are: 1234567890abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!%&-~@#$^*
• Invalid characters: ><?</td></tr>
<tr><td>My Identity Type</td><td>Options are:
• IP (default) — The My Identity - IP field appears with the WAN IP address assigned by the carrier
• FQDN — The My Identity - FQDN field appears. Enter a fully qualified domain name (FQDN) e. g., modemname.domainname.com
• User FQDN — The My Identity - FQDN field appears. Enter a User FQDN whose values should include a username (e.g. user@domain.com)</td></tr>
<tr><td>My Identity - IP or My Identity - FQDN</td><td>• My Identity - IP appears only when IP is selected from the My Identity Type drop-down menu. The WAN IP address assigned by the carrier appears.
• My Identity - FQDN appears only when User FQDN or FQDN is selected from the My Identity Type drop-down menu. Enter an FQDN or User FQDN.

Note: If you are using a FQDN for your device (My Identity) either:
• Set up a Dynamic DNS on the Services > Dynamic DNS tab. (See Dynamic DNS on page 142.) or
• Use a DNS server as your domain host</td></tr>
<tr><td>Peer Identity Type</td><td>Required in some configurations to identify the client or peer side of a VPN connection. Options are:
• IP (default) — The Peer Identity - IP field appears with the IP address of a VPN server set up by Sierra Wireless for your testing purposes
• FQDN — The Peer Identity - FQDN field appears. Enter an FQDN (e. g. modemname.domainname.com)
• User FQDN — The Peer Identity - FQDN field appears. Enter a User FQDN whose values should include a username (e.g., user@domain.com)</td></tr>
</table>

Field	Description
Peer Identity - IP or **Peer Identity - FQDN**	• Peer Identity - IP appears only when IP is selected from the Peer Identity Type drop-down menu. The VPN Gateway IP Address appears. • Peer Identity - FQDN appears only when User FQDN or FQDN is selected from the Peer Identity Type drop-down menu. Enter the Peer FQDN or Peer User FQDN.
Negotiation Mode	Enable this configuration to operate the onboard VPN under Aggressive mode. Aggressive mode offers increased performance at the expense of security. Options are: • Main (default) • Aggressive
IKE Encryption Algorithm	Determines the type and length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets. 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption. Options are: DES, 3DES, AES-128 (default), and AES-256
IKE Authentication Algorithm	MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests. Options are: MD5, SHA1 (default), and SHA256
IKE Key Group	Options are: DH1, DH2 (default), or DH5
IKE SA Life Time	Determines how long the VPN tunnel is active in seconds. Options are: 180 to 86400; Default: 7200
IKE DPD	Dead Peer Detection (DPD) Options are: • Disable (default) • Enable When DPD is enabled, the AirLink gateway checks to see if the server is still present if there has been no traffic for a configured interval. If it does not receive an acknowledgment, it retries at 5 second intervals. If there is no acknowledgment after 5 retries, the status of the VPN is set to Not Connected and the device attempts to renegotiate IPSEC security parameters with its peer. Default is Disabled. *Note: Sierra Wireless recommends that you Enable IKE DPD. Otherwise the AirLink gateway has no way of detecting that the connection to the VPN server is still available.*
IKE DPD Interval (seconds)	Use this field to set the DPD interval (in seconds). If there has been no traffic for the period of time set in this field, the AirLink gateway retries checking with the server, as described in IKE DPD. Options are: 0 to 3600 (default is 1200) If this field is set to 0, DPD monitoring is turned off (or disabled as described in the IKE DPD section), but the AirLink gateway still responds to DPD requests from the server.
Local Address Type	The network information of the device. Options are: Use the Host Subnet, Single Address, and Subnet Address (default)
Local Address	Device subnet address
Local Address - Netmask	Device subnet mask information Default: 255.255.255.0

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Remote Address Type</td><td>The network information of the IPsec server behind the IPsec gateway.
Options are: Subnet Address (default) and Single Address</td></tr>
<tr><td>Remote Address</td><td>The IP address or subnet of the device(s) connected to the gateway
If the remote address is 0.0.0.0, the remote address netmask should also be 0.0.0.0.
Note that you can only have one remote address of 0.0.0.0 for all the VPNs.
Default values are:
<table><tr><th>VPN</th><th>Remote Address</th></tr><tr><td>1</td><td>10.11.12.0</td></tr><tr><td>2</td><td>10.11.13.0</td></tr><tr><td>3</td><td>10.11.14.0</td></tr><tr><td>4</td><td>10.11.15.0</td></tr><tr><td>5</td><td>10.11.16.0</td></tr></table></td></tr>
<tr><td>Remote Address - Netmask</td><td>Remote subnet mask information
Default: 255.255.255.0
0.0.0.0 is allowed for the remote address subnet mask as long as the remote address is also 0.0.0.0.</td></tr>
<tr><td>Perfect Forward Secrecy</td><td>Provides additional security through a DH shared secret value. When this feature is enabled, one key cannot be derived from another. This ensures previous and subsequent encryption keys are secure even if one key is compromised. Options are: Yes (default) or No.</td></tr>
<tr><td>IPsec Encryption Algorithm</td><td>Determines the type and length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets. 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption.
Options are: None, DES, 3DES, AES-128 (default), and AES-256.</td></tr>
<tr><td>IPsec Authentication Algorithm</td><td>Can be configured with MD5 or SHA1. MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests.
Options are: None, MD5, SHA1 (default), and SHA 256.</td></tr>
<tr><td>IPsec Key Group</td><td>Determines how the AirLink gateway VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during the phase 1 authentication. The AirLink gateway supports three prime key lengths, including Group 1 (768 bits), Group 2 (1,024 bits), and Group 5 (1,536 bits). Options are: None, DH1, DH2 (default), or DH5.</td></tr>
<tr><td>IPsec SA Life Time</td><td>Determines how long the VPN tunnel is active in seconds
Options are: 180 to 86400; Default: 7200</td></tr>
<tr><td colspan="2">Additional Remote Subnets</td></tr>
<tr><td>Remote Subnet 2 Address type</td><td>The network information for subnet 2 IPsec server behind the IPsec gateway.
Options are: Subnet Address (default) and Single Address</td></tr>
<tr><td>Remote Subnet 2 Address</td><td>The IP address for the subnet 2 device behind the gateway</td></tr>
</table>

Field	Description
Remote Subnet 2 Address - Netmask	Remote subnet 2 mask information Default: 255.255.255.0
Remote Subnet 3 Address type	The network information for subnet 3 IPsec server behind the IPsec gateway. Options are: Subnet Address (default) and Single Address
Remote Subnet 3 Address	The IP address for the subnet 3 device behind the gateway
Remote Subnet 3 Address - Netmask	Remote subnet 3 mask information Default: 255.255.255.0

GRE Tunnel

The AirLink gateway can act as a Generic Routing Encapsulation (GRE) endpoint, providing a means to encapsulate a wide variety of network layer packets inside IP tunneling packets. With this feature you can reconfigure IP architectures without worrying about connectivity. GRE creates a point-to-point link between routers on an IP network.

To configure GRE:

1. In ACEmanager, go to VPN.
2. Select the VPN you want to configure (1, 2, 3, 4, or 5).
3. In the VPN Type field, select GRE. The screen expands to show the GRE fields.

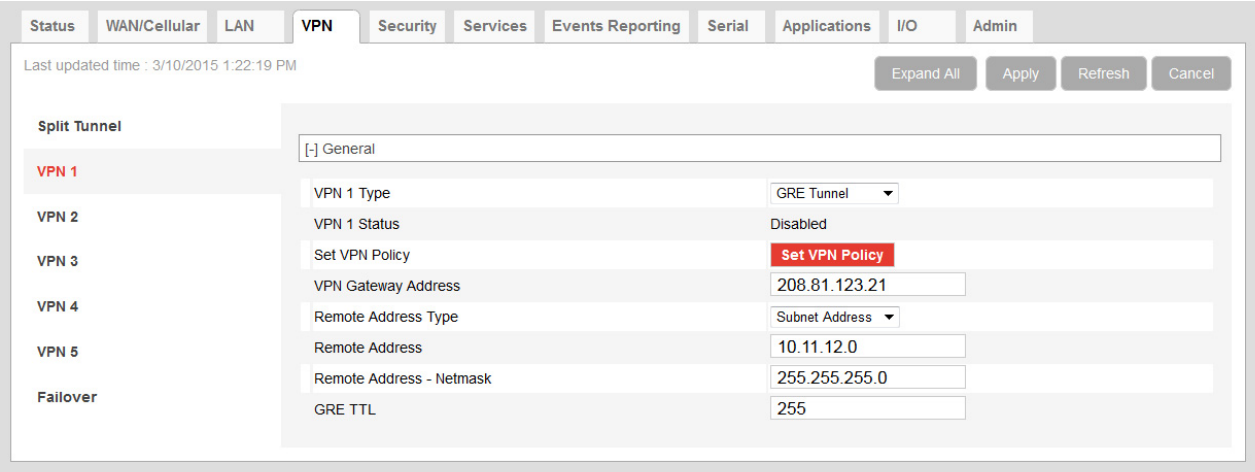


Figure 6-3: ACEmanager: VPN > VPN1 > GRE Tunnel

4. See the following table for instructions on completing the GRE fields.

5. Once the configuration is complete, either:
   - Click the Set VPN Policy button.

   Or
   - Reboot the AirLink gateway.

Field	Description
VPN # Type	Options are: Tunnel Disabled or GRE Tunnel. Enabling the GRE Tunnel will expose other options for configuring the tunnel.
VPN # Status	Indicates the status of the GRE tunnel on the device Options are: Disabled, Connected or Not Connected
Set VPN Policy	After completing the VPN Configuration: 1. Click this button to apply the new settings (or reboot the device). 2. Check the VPN Status field to confirm the status of the VPN connection. (See VPN # Status.)
VPN Gateway Address	The IP address of the device that this client connects to. This IP address must be open to connections from the device.
Remote Address Type	The network information of the GRE server behind the GRE gateway
Remote Address	The IP address of the device behind the gateway
Remote Address - Netmask	The subnet network mask of the device behind the GRE gateway *Note: Never use a 16-bit subnet mask: GRE tunnel establishment will fail.*
GRE TTL	GRE time to live (TTL) value is the upper bound on the time that a GRE packet can exist in a network. In practice, the TTL field is reduced by one on every router hop. This number is in router hops and not in seconds.

SSL Tunnel

Note: SSL Tunnel configuration is only available on VPN 1.

The SSL tunnel is implemented using OpenVPN. OpenVPN uses SSL/TLS to facilitate key exchange and supports up to 256-bit encryption. OpenVPN is capable of crossing network address translators (NATs) and firewalls. Peers can authenticate each other using pre-shared keys, certificates, or username and password.

The AirLink gateway client authenticates the server using a PKI certificate. The server likewise authenticates the client. The Root CA certificate for the server certificate must be loaded on the device.

To configure an SSL VPN tunnel:

1. In ACEmanager, go to VPN.
2. Select the VPN 1.
3. In the VPN Type field, select SSL Tunnel. The screen expands to show the SSL Tunnel fields.

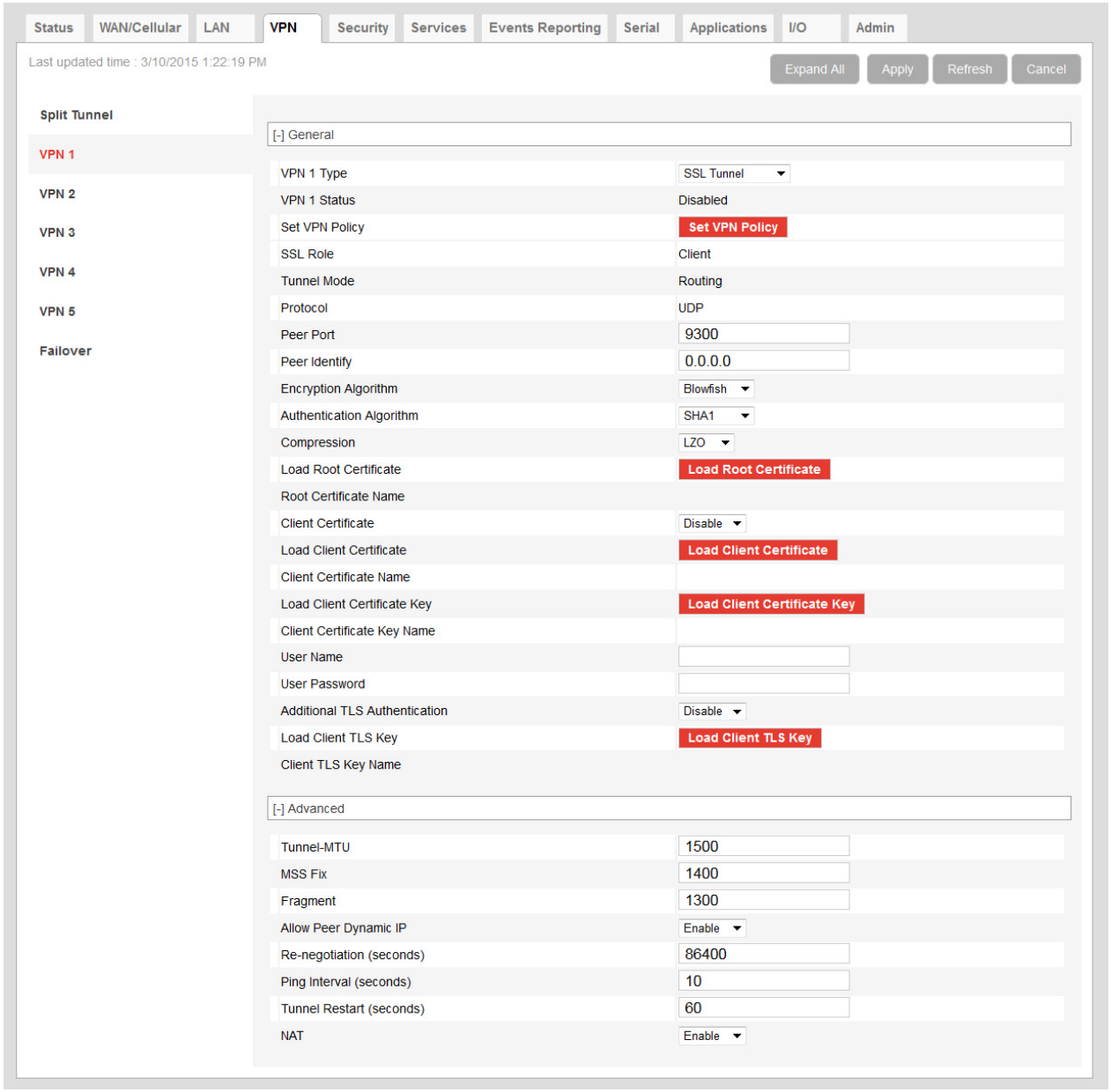


Figure 6-4: ACEmanager: VPN > VPN1 > SSL Tunnel

4. See the following table for instructions on completing the SSL Tunnel fields.
5. Once the configuration is complete, either:
   - Click the Set VPN Policy button.

   Or
   - Reboot the AirLink gateway.

Field	Description
General	
VPN 1 Type	Options are: Tunnel Disabled or SSL Tunnel. Enabling the SSL Tunnel will expose other options for configuring the tunnel.
VPN 1 Status	Indicates the status of the SSL tunnel on the device Options are: Disabled, Connected or Not Connected
Set VPN Policy	After completing the VPN Configuration: 1. Click this button to apply the new settings (or reboot the device). 2. Check the VPN Status field to confirm the status of the VPN connection. (See VPN 1 Status.)
SSL Role	The AirLink gateway can only be an SSL client. Default: Client
Tunnel Mode	The Tunnel Mode is set to “Routing”.
Protocol	Displays the protocol used for configuration. Only supports UDP
Peer Port	The Peer Port is the UPD port on the peer device.
Peer Identity	Enter the IP address or Fully Qualified Domain Name (FQDN) of the peer device.
Encryption Algorithm	Options are: DES, Blowfish, DES, Cast128, AES-128, and AES-256
Authentication Algorithm	Options are: MD5, SHA-1, and SHA-256
Compression	Options are: LZ0 or NONE
Load Root Certificate	Loads the server root CA (Certificate Authority) certificate When you click the button, a window pops up and enables you to browse and select the file containing the root CA certificate.
Root Certificate Name	Displays the name of the most recently uploaded root certificate
Client Certificate	Enables or disables use of a client certificate.
Load Client Certificate	This field appears only if Client Certificate is enabled. Loads the client certificate When you click the button, a window pops up and enables you to browse and select the file containing the client certificate.
Client Certificate Number	Displays the number of the most recently uploaded client certificate.
Load Client Certificate Key	This field appears only if Client Certificate is enabled. Loads the client certificate key When you click the button, a window pops up and enables you to browse and select the file containing the client certificate key.
Client Certificate Key Name	Displays the name of the most recently uploaded client certificate key
User Name	The user name required for client authentication
User Password	The user password required for client authentication

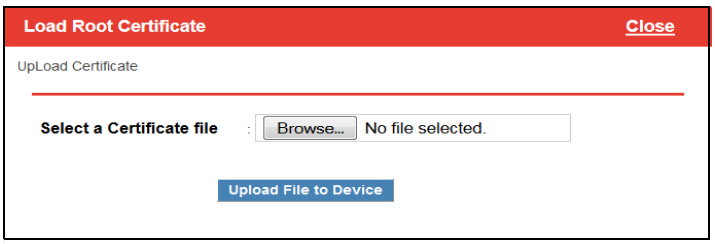
Field	Description
Additional TLS Authentication	Enables or disables use of Transport Layer Security (TLS) authentication.
Load Client TLS Key	This field appears only if Additional TLS Authentication is enabled. Loads the client TLS key When you click the button, a window pops up and enables you to browse and select the file containing the client TLS key.
Client TLS Key Name	Displays the name of the most recently uploaded client TLS key
Advanced	
Tunnel-MTU	Default: 1500 bytes
MSS Fix	Default: 1400 bytes
Fragment	Default: 1300 bytes
Allow Peer Dynamic IP	Options are: Enable or Disable
Re-negotiation (seconds)	Default: 86400 (24 hours)
Ping Interval (seconds)	This is the keep-alive sent by the client. Default: 0 seconds
Tunnel Restart (seconds)	Enter the time for a tunnel restart (unit in seconds)
NAT	Options are: Enable or Disable. Note that this is a Carrier NAT, not a local NAT

Load Root Certificate

Note: The process is similar for uploading the client certificate, the client certificate key and the client TLS key.

To load a root certificate:

1. Click Load Root Certificate.
   The following dialog-box appears.



2. Select the appropriate file for your device.
3. Click Upload File to Device.

VPN Failover

VPN Failover is only available for IPsec VPN tunnels. To use this feature, configure a primary and a secondary VPN tunnel. Dead Peer Detection (DPD) verifies the status of the primary connection. If the primary VPN goes down (i.e. DPD detects that the end device is not responding) traffic is automatically switched to the secondary (backup) VPN tunnel. DPD continues to ping the primary VPN responder. If configured to do so, once the primary VPN tunnel is up, traffic automatically reverts to the primary VPN. Status fields in the ACEmanager UI inform you of the current status of the two VPNs. Figure 6-5 shows a typical configuration.

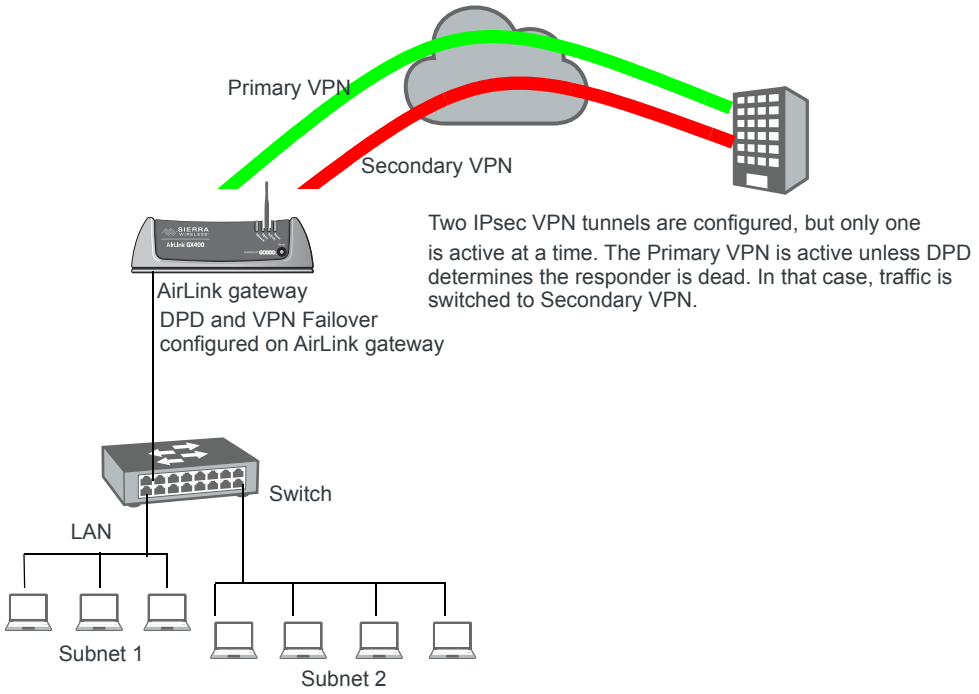


Figure 6-5: VPN Failover Configuration

To configure VPN Failover:

1. Configure two IPsec VPN tunnels. The one you want to designate as the Primary VPN must have Dead Peer Detection configured. For the Secondary VPN, you only need to configure the remote gateway address. For other settings, such as the local and remote subnets, the secondary VPN uses the same settings as the primary VPN.

   For instructions on configuring IPsec VPN tunnels, see IPsec Tunnel on page 111.
2. Go to VPN > Failover and configure the first three fields. See the table following the screen shot for details.
3. Click Apply and reboot the AirLink gateway.

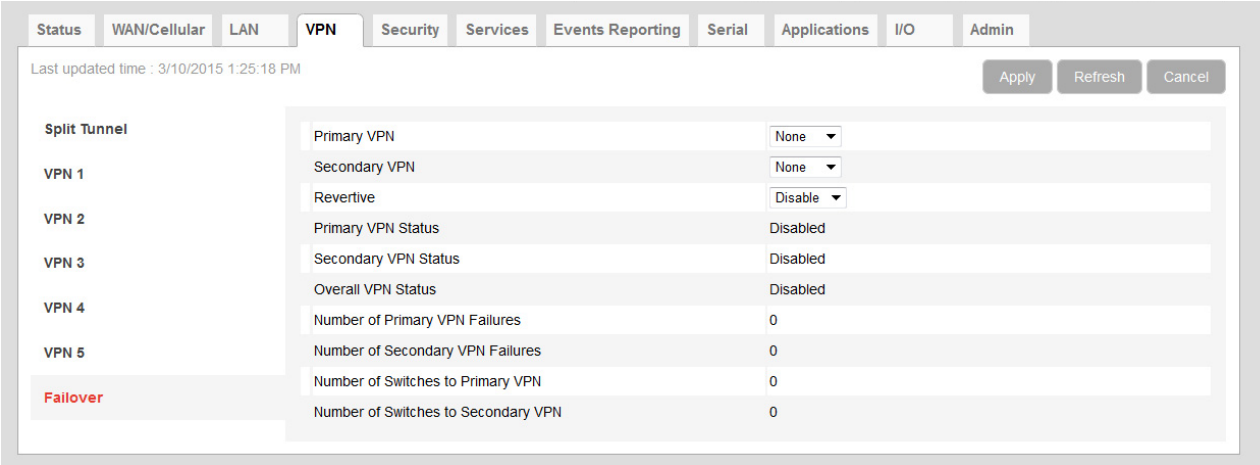


Figure 6-6: ACEmanager: VPN > Failover

Field	Description
Primary VPN	ID of the Primary VPN (for VPN Failover) i.e. VPN 1, VPN 2, VPN 3, VPN 4, VPN 5, or None (None is the default.)
Secondary VPN	ID of the Secondary VPN (for VPN Failover) i.e. VPN 1, VPN 2, VPN 3, VPN 4, VPN 5, or None (Default is None.)
Revertive	When VPN Failover is configured and this field is set to Enable, traffic automatically switched from the Secondary VPN back to the Primary VPN when the failure is resolved and the Primary VPN tunnel is up again. Options are • Enable (default) • Disable
Primary VPN Status	Status of the Primary VPN: • Disabled—VPN Failover is disabled. (default) • Connecting—The VPN is trying to connect to the responder. • Active—The VPN tunnel is ready and transferring traffic. • Backup—This is currently the backup VPN connection. • Failed—Dead Peer Detection (DPD) has determined that the VPN responder is dead, or a ping sent to the VPN host failed. • Out of Service—There have been 5 DPD failures within an hour.
Secondary VPN Status	Status of the Secondary VPN: • Disabled—VPN Failover is disabled. (default) • Connecting—The VPN is trying to connect to the responder. • Active—The VPN tunnel is ready and transferring traffic. • Backup—This is currently the backup VPN connection. • Failed—Dead Peer Detection (DPD) has determined that the VPN responder is dead, or a ping sent to the VPN host failed. • Out of Service—There have been 5 DPD failures within an hour.

Field	Description
Overall VPN Status	Status of the overall VPN: • Disabled—VPN Failover is disabled. (default) • Connecting—One of the VPNs is trying to connect to the responder. • Active—One VPN tunnel is currently in use. The backup VPN is available. • Backup_Unavailable—One VPN tunnel is currently in use. The backup VPN is not available. • Out of Service—Neither the primary nor secondary VPN is operational. • N/A—The overall VPN status is temporarily not available. Click Refresh.
Number of Primary VPN Failures	Number of times DPD has failed on the Primary VPN since the device has been rebooted or the “Set VPN Policy” button was clicked
Number of Secondary VPN Failures	Number of times DPD has failed on the Secondary VPN since the device has been rebooted or the “Set VPN Policy” button was clicked
Number of Switches to Primary VPN	Number of times traffic was switched to the Primary VPN since the device has been rebooted or the “Set VPN Policy” button was clicked
Number of Switches to Secondary VPN	Number of times traffic was switched to the Secondary VPN since the device has been rebooted or the “Set VPN Policy” button was clicked

7: Security Configuration

The Security tab covers firewall-type functions. These functions include how data is routed or restricted from one side of the device to the other, i.e., from computers or devices connected to the device (LAN) and from computers or devices contacting it from a remote source (WAN). These features are set as rules.

Tip: *For additional security, Sierra Wireless recommends that you change the default password for ACEmanager. See Change Password on page 224.*

Solicited vs. Unsolicited

How the device responds to data being routed from one network connection to the other depends on the origin of the data.

- If a computer on the LAN initiates a contact to a WAN location (such as a LAN connected computer accessing an Internet web site), the response to that contact is solicited.
- If, however, a remote computer initiates the contact (such as a computer on the Internet accessing a camera connected to the device), the connection is considered unsolicited.

Port Forwarding

In Port Forwarding, any unsolicited data coming in on a defined Public Port is routed to the corresponding Private Port and Host IP of a device connected to the specified Physical Interface. You can forward a single port or a range of ports.

Note: Port Forwarding requires Private Mode. See Private and Public Mode on page 79.

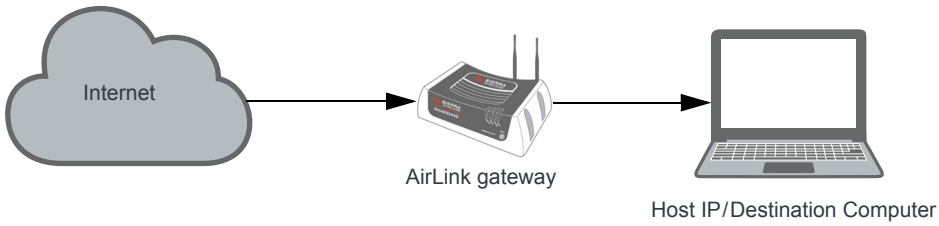


Figure 7-1: Port Forwarding

Note: You can set up a maximum of 48 port forwarding rules, 24 on the Port Forwarding screen and an additional 24 on the Extended Port Forwarding screen.

Single port

To define a port forwarding rule for a single port:

1. In ACEmanager, go to Security > Port Forwarding.

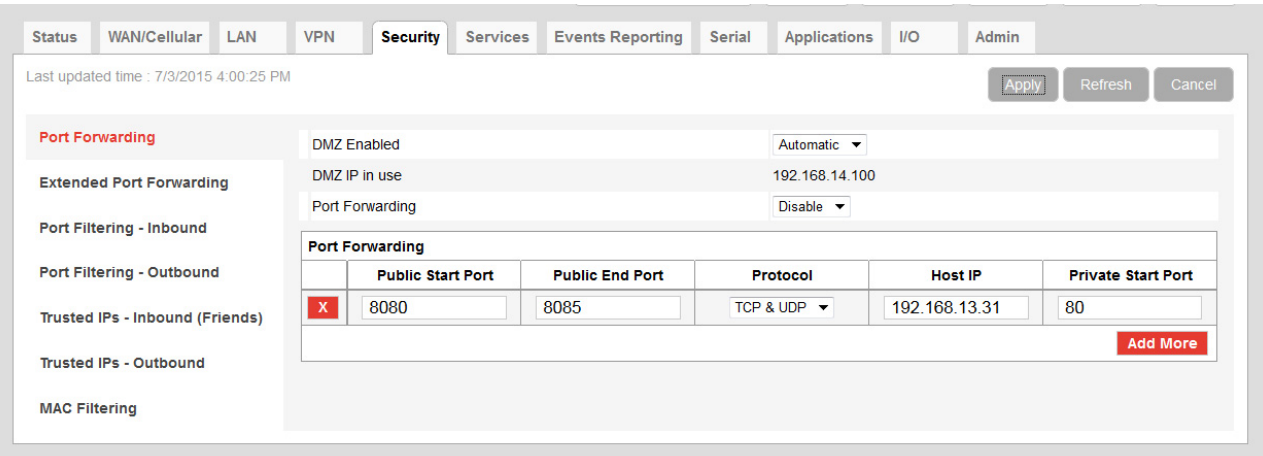


Figure 7-2: ACEmanager: Security > Port Forwarding (Single Port)

2. In the Port Forwarding field, select Enable.
3. Click “Add More” to display a rule line.
4. In the Public Start Port field, enter the desired public network port number. Values between 1 and 65535 are supported, although Sierra Wireless recommends using a value greater than 1024.

   Unsolicited data coming in on this port is forwarded to the port you select in the Private Start Port field.
5. In the Public End Port field, enter 0.
6. Select the desired protocol (see Protocol on page 130):
   - TCP
   - UDP
   - TCP & UDP
7. Enter the IP address of the computer you want to forward data to.
8. In the Private Start Port field, enter the number of the port on the destination computer that you want to forward data to.
9. Click Apply.

   The Port Forwarding screen allows for 24 port forwarding rules.
10. Optional—If you need additional port forwarding rules, click Extended Port Forwarding on the left menu, and continue adding rules, up to a total over both screens of 48.

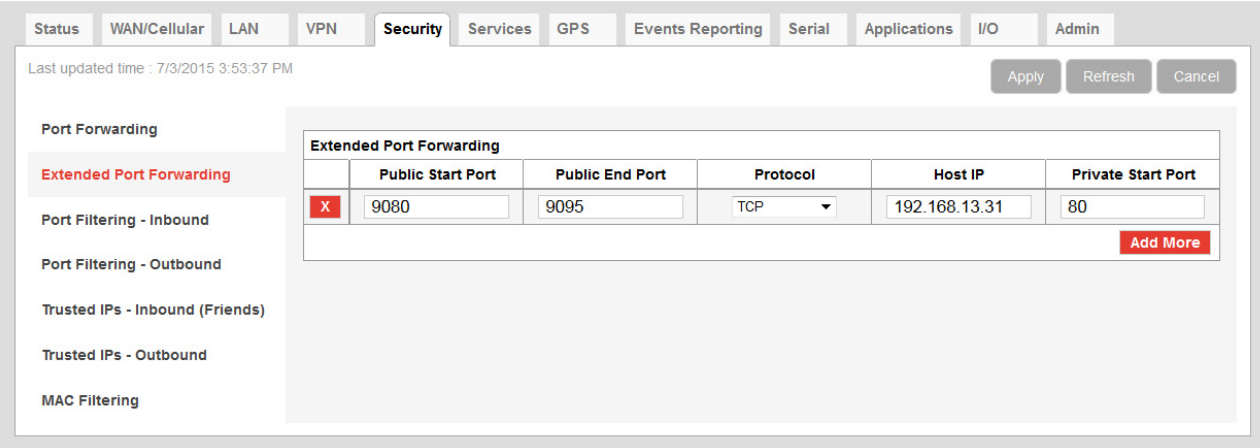


Figure 7-3: ACEmanager: Security > Extended Port Forwarding

11. Reboot.

You do not need to reboot immediately, if you have additional changes to make, but port forwarding does not take effect until the device is rebooted.

Range of ports

To define a port forwarding rule for a range of ports:

1. In ACEmanager, go to Security > Port Forwarding.

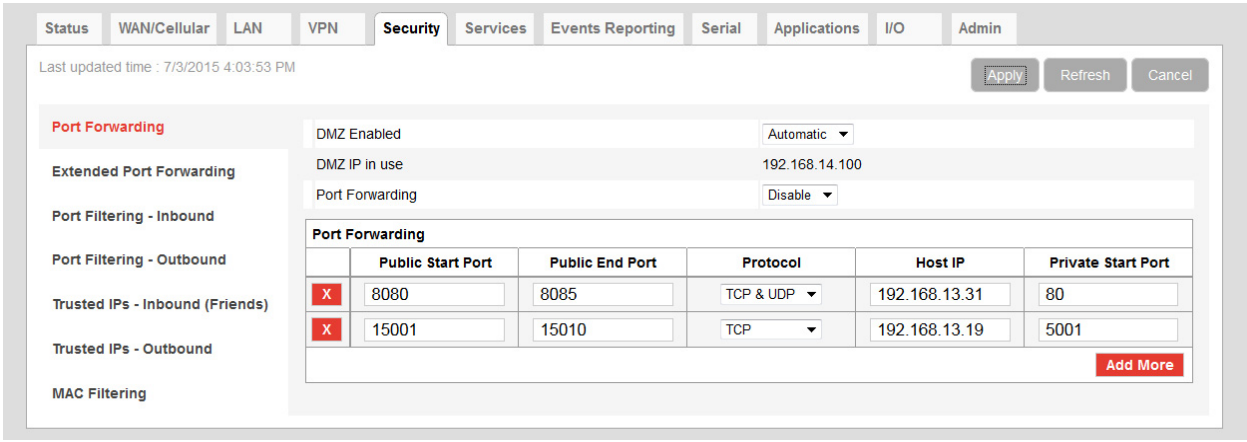


Figure 7-4: ACEmanager: Security > Port Forwarding (Port Range)

2. In the Port Forwarding field, select Enable.

3. Click “Add More” to display a rule line.

4. Set the port range for incoming data:

a. In the Public Start Port field, enter the desired public network port number. Values between 1 and 65535 are supported, although Sierra Wireless recommends using a value greater than 1024.

b. In the Public Port End field, enter the last public network port number in the range. The value you enter in the Public Port End field must be greater than the value in the Public Start Port field, or ALEOS rejects the selection.

Unsolicited data coming in on ports in this range are forwarded to a range of ports, starting with the port you select in the Private Start Port field.

5. Select the desired protocol (see Protocol on page 130):
   - TCP
   - UDP
   - TCP & UDP
6. Enter the IP address of the computer you want to forward data to.

   To forward a port to a local ALEOS Service, set the Host IP to 127.0.0.1.
7. In the Private Start Port field, enter the starting port number for the range of ports on the destination computer that you want to forward data to.
8. Click Apply.

   The Port Forwarding screen allows for 24 port forwarding rules.
9. Optional—If you need additional port forwarding rules, click Extended Port Forwarding on the left menu, and continue adding rules, up to a total over both screen of 48.

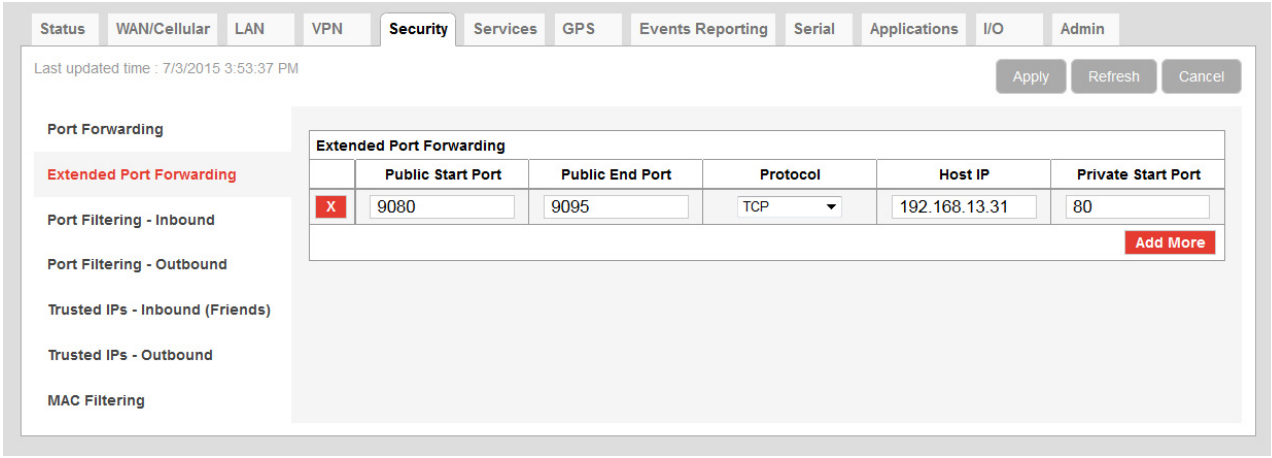


Figure 7-5: ACEmanager: Security > Extended Port Forwarding

10. Reboot.

    You do not need to reboot immediately, if you have additional changes to make, but port forwarding does not take effect until the device is rebooted.

Note: Sierra Wireless recommends that the total number of port forwardings be fewer than 1000 ports, including single port forwarding and port forwarding within a range.

Field	Description
Port Forwarding	Enables port forwarding rules. Options are Enable and Disable (default).
Public Start Port	Port on the public network or starting port on the public network for a range of ports. • Supported values: 1–65535 (Recommended values: greater than 1024)

Field	Description
Public End Port	Ending port for a range of ports on the public network. • For a single port forwarding, this field must be 0. • For a range of ports, this value must be greater than the value in the Public Start Port field.
Protocol	The protocol to be used with the forwarded port: • TCP—Only those unsolicited data requests using TCP are forwarded • UDP—Only those unsolicited data requests using UDP are forwarded • TCP & UDP—Unsolicited data requests using either TCP or UDP are forwarded
Host IP	IP address of the computer (or device) you want to forward data to.
Private Start Port	Port on the destination computer used as the port for single port forwarding rules, or as the start port for a port forwarding range.

Port Forwarding Example

The following example shows you how to configure a port forward rule for a range of 6 ports on an Ethernet-connected device:

1. In ACEmanager, go to Security > Port Forwarding, and enable Port Forwarding.
2. Click “Add More” to display a rule line.
3. Enter 8080 for the Public Start Port.
4. Enter 8085 for the Public End Port.
5. Select TCP & UDP.
6. Enter 192.168.13.30 as the Host IP.
7. Enter 80 as the Private Start Port.

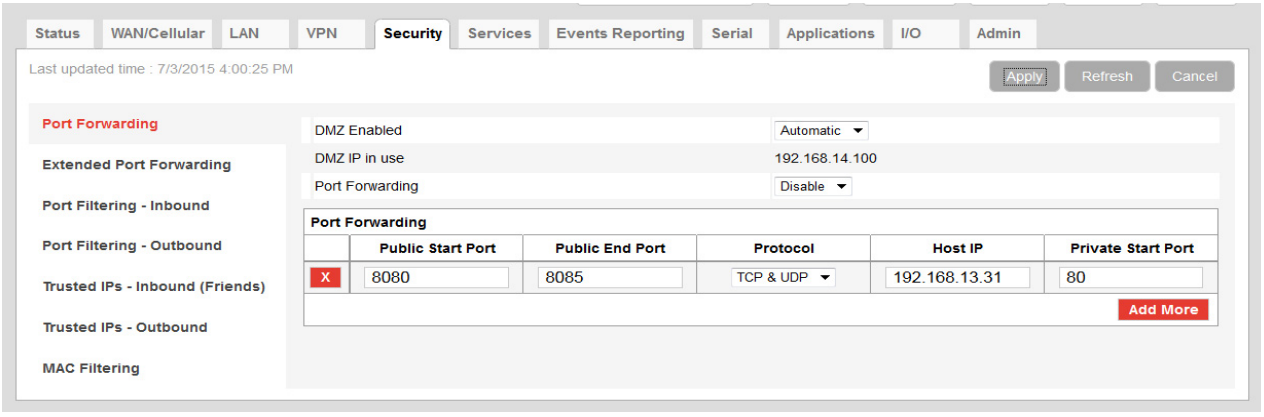


Figure 7-6: ACEmanager: Port Forwarding example

8. Click Apply.
9. Reboot.

   You do not need to reboot immediately, if you have additional changes to make, but port forwarding does not take effect until the device is rebooted.

An unsolicited TCP and UDP data request coming in to the AirLink gateway on port 8080 is forwarded to the LAN connected device, 192.168.13.30, at port 80. In addition, unsolicited data requests coming in from the Internet on ports 8081, 8082, 8083, 8084, and 8085 are forwarded to ports 81, 82, 83, 84, and 85 respectively.

DMZ

The DMZ is used to direct unsolicited inbound traffic to a specific LAN device such as a computer running a web server or other internal application. The DMZ with public mode is particularly useful for certain services like VPN, NetMeeting, and streaming video where the remote server may require a WAN connection to the LAN device rather than being NATed by the router. In public mode unsolicited traffic to hosts in the DMZ is permitted by default.

Options for DMZ are Automatic, Manual, and Disable.

Automatic uses the first connected host. If more than one host is available (multiple Ethernet on a switch connected to the device and/or Ethernet with USBnet) and you want to specify the host to use as the DMZ, select Manual and enter the IP address of the desired host.

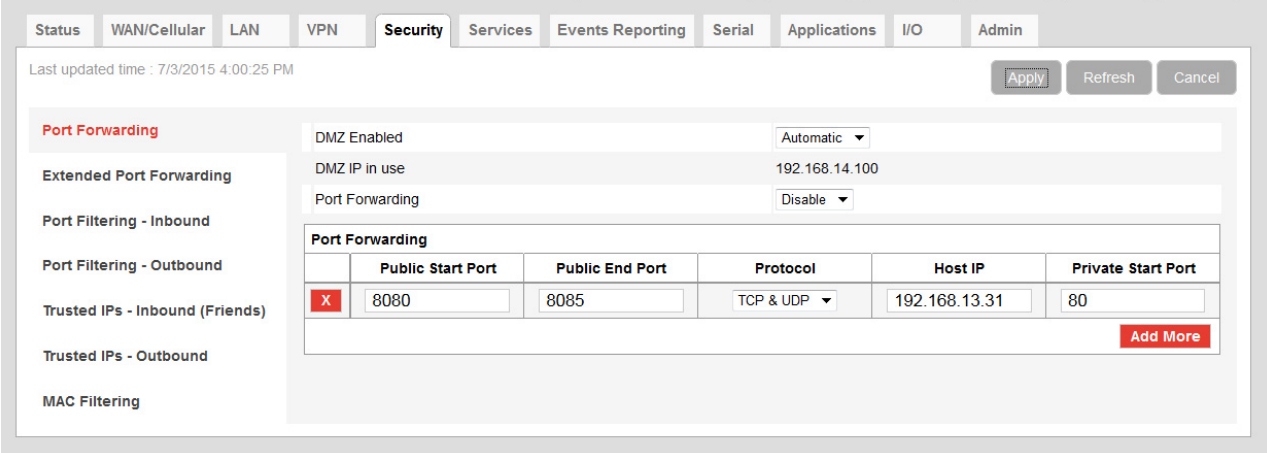


Figure 7-7: ACEmanager: Security > Port Forwarding (DMZ)

Field	Description
DMZ Enabled	The AirLink gateway allows a single client to connect to the Internet through a demilitarized zone (DMZ). Options are: • Automatic—enables the first connected host or the Public Mode interface as the DMZ • Manual—inserts a specific IP address in the DMZ IP field • Disable—no connected host receives unsolicited traffic from the cellular network or Internet (default)

Field	Description
DMZ IP	This field only appears if Manual is selected for the DMZ Enabled field; this field does not display if the DMZ is disabled. This is the IP address of the private mode host that should be used as the DMZ.
DMZ IP in use	IP address of the host to which inbound unsolicited packets are sent When the device passes the Network IP to the configured public host, the DMZ IP in Use displays the public IP.

Example of configuring the DMZ on an Ethernet connected device, using the settings shown in Figure 7-7:

1. Enter 192.168.13.100 for the DMZ IP.
2. Select Ethernet as the Default Interface.

An unsolicited data request coming in to the AirLink gateway on any port is forwarded to the LAN device, 192.168.13.100, at the same port.

Note: The DMZ settings are independent of the number of Port Forward entries and can be used with port forwarding to pass anything not forwarded to specific ports.

Port Filtering—Inbound

Port Filtering—Inbound restricts unsolicited access to the AirLink gateway and all LAN-connected devices.

You can enable Port Filtering to either block or allow specified ports. When enabled, all ports not matching the rule are allowed or blocked depending on the mode.

You can configure Port Filtering either on individual ports or for a range of ports. Click Add More for each port filtering rule you want to add.

Note: Inbound restrictions do not apply to responses to outbound data requests. To restrict outbound access, you need to set the applicable outbound filter.

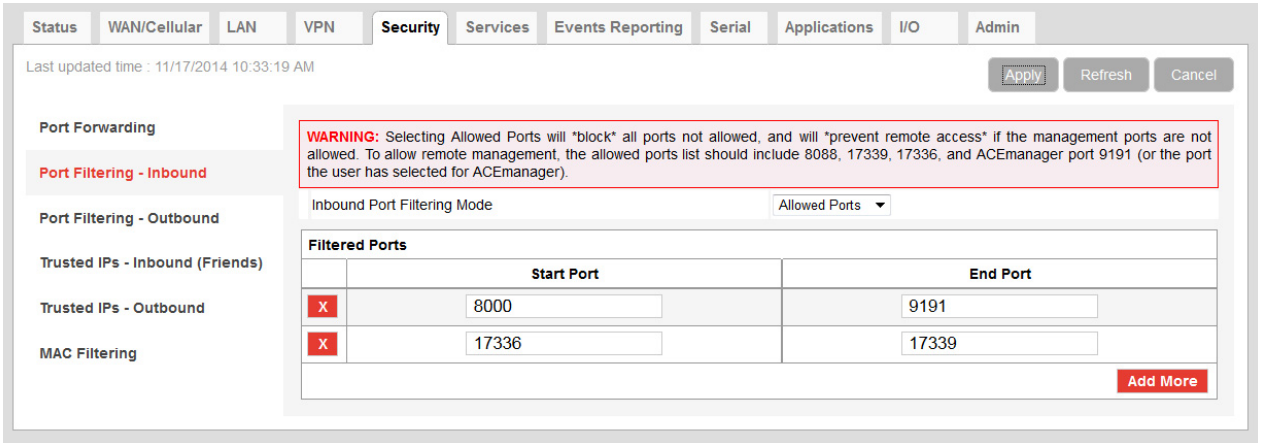


Figure 7-8: ACEmanager: Security > Port Filtering - Inbound

Field	Description
Inbound Port Filtering Mode	Options are: • Disable (default) • Blocked Ports—ports though which traffic is blocked (Shown in Filtered Ports list) • Allowed Ports—ports through which traffic is allowed (Shown in Filtered Ports list)
Filtered Ports	
Start Port	A single port or the first port in a range of ports on the public network (mobile network accessible)
End Port	The end of the range on the public network (mobile network accessible).

Warning: *Selecting Allowed Ports will *block* all ports not allowed, and will *prevent remote access* if the management ports are not allowed. To allow remote management, the allowed ports list should include 8088, 17339, 17336, and ACEmanager port 9191 (or the port you selected for ACEmanager).*

Port Filtering — Outbound

Port Filtering—Outbound restricts LAN access to the external network, i.e., the Internet.

Port Filtering can be enabled to block ports specified or allow specified ports. When enabled, all ports not matching the rule will be allowed or blocked depending on the mode.

Port Filtering can be configured on individual ports or for a range of ports. Click Add More for each port filtering rule you want to add.

Note: Outbound restrictions do not apply to responses to inbound data requests. To restrict inbound access, you need to set the applicable inbound filter.

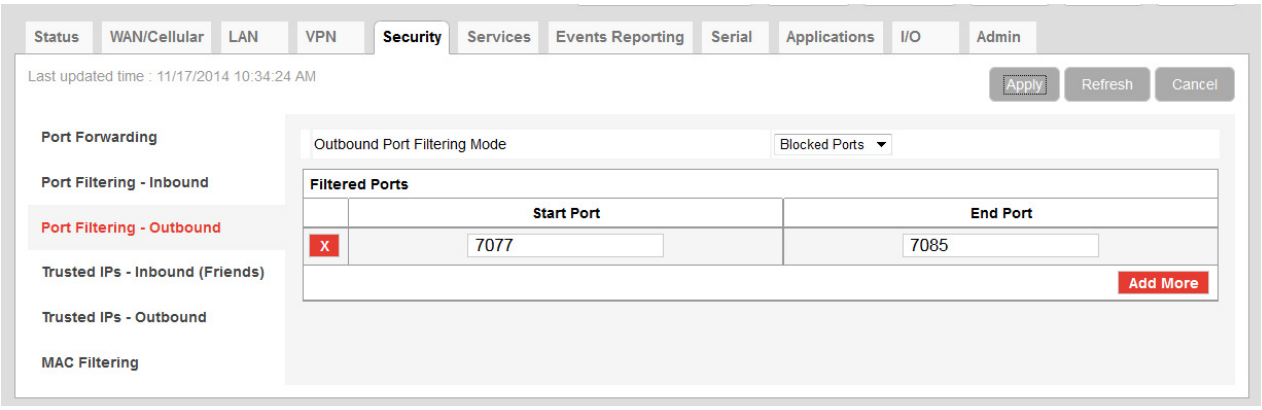


Figure 7-9: ACEmanager: Security > Port Filtering - Outbound

Field	Description
Outbound Port Filtering Mode	Allowed and blocked ports through which traffic is either allowed or blocked (respectively) are listed. Options are: • Disable (default) • Blocked Ports—ports though which traffic is blocked (Shown in Filtered Port s list) • Allowed Ports—ports through which traffic is allowed (Shown in Filtered Port s list) *Note: Outbound IP filter supports up to 9 ports.*
Start Port	The first of a range or a single port on the LAN
End Port	The end of the range on the LAN

Trusted IPs—Inbound (Friends)

Trusted IPs—Inbound restricts unsolicited access to the AirLink gateway and all LAN connected devices.

Tip: *Trusted IPs-Inbound was called Friends List in legacy AirLink products.*

When enabled, only packets with source IP addresses matching those in the list or range of trusted hosts will have unrestricted access to the AirLink gateway and/or LAN connected devices.

Note: Inbound restrictions do not apply to responses to outbound data requests. To restrict outbound access, you need to set the applicable outbound filter.

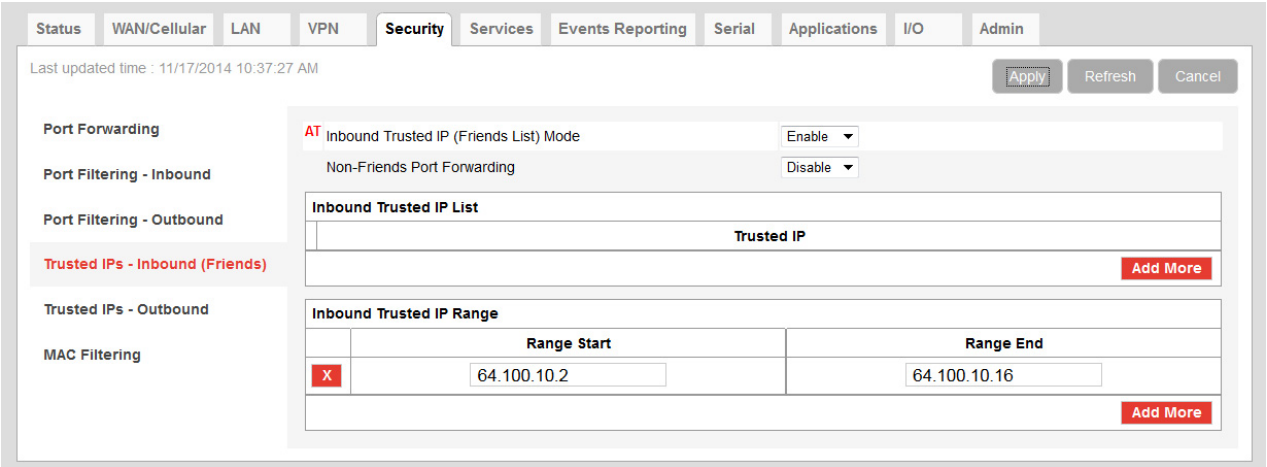


Figure 7-10: ACEmanager: Security > Trusted IPs > Inbound (Friends)

Field	Description
Inbound Trusted IP (Friends List) Mode	Disables or Enables port forwarding rules. Options are Disable (default) or Enable.
Non-Friends Port Forwarding	Non-Friends port forwarding is like an allow rule for any of the forwarded ports. If it is enabled, the port forwarding rules apply to all incoming packets. If it is disabled, only Inbound Trusted List (or Range) IPs get through. Options are Disable (default) or Enable.
Inbound Trusted IP List	Enter a single trusted IP address: for example 64.100.100.2. Click Add More to add additional IP addresses to the list.
Inbound Trusted IP Range	Use this section of the page to enter a range of trusted IP addresses.
Range Start	Specify the start and end IP addresses for the trusted IP address range, for example, entering 64.100.10.2 as the Range Start and 64.100.10.15 as the Ranges End would allow 64.100.10.5 but would not allow 64.100.10.16.
Range End	

Trusted IPs—Outbound

Trusted IPs—Outbound restricts LAN access to the external network (Internet).

When enabled, only packets with the destination IP addresses matching those in the list of trusted hosts will be routed from the LAN to the external location.

Note: Outbound restrictions do not apply to responses to inbound data requests. To restrict inbound access, you need to set the applicable inbound filter.

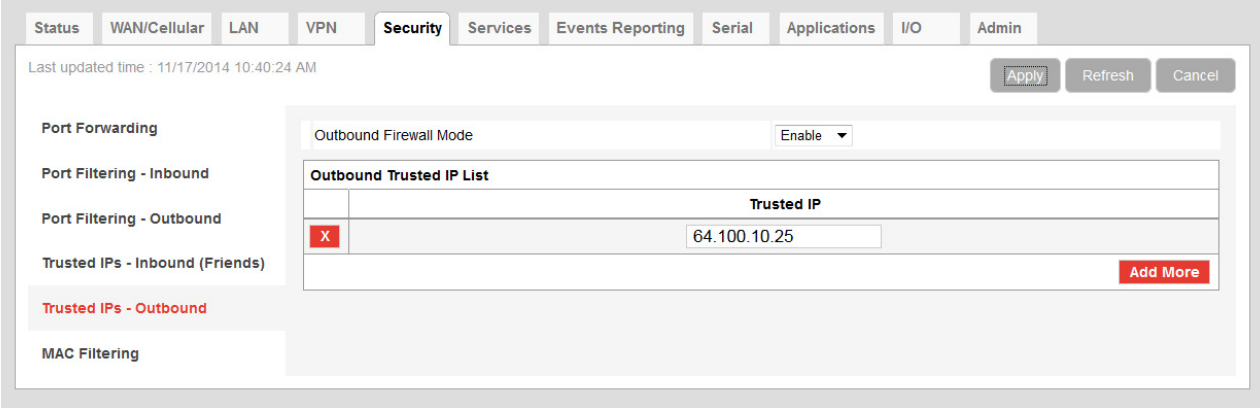


Figure 7-11: ACEmanager: Security > Trusted IPs - Outbound

Field	Description
Outbound Firewall Mode	Disables or enables the Outbound Firewall Options are: • Disable (default)—Allows all outbound traffic • Enable—Only outbound traffic destined for an IP address on the Trusted IP list is allowed. All other outbound traffic is blocked.
Outbound Trusted IP List	Each entry can be configured to allow a single IP address (e.g., 64.100.100.2) Click Add More to add additional IP addresses to the list.

MAC Filtering

MAC filtering restricts LAN connection access. You can create a list of up to 20 devices that are allowed a connection based on their MAC address. When MAC filtering is enabled, devices not on the allowed list are explicitly blocked. Hosts directly connected to the device but not in the Allowed list may show an active physical connection, but are blocked from sending traffic of any kind to the device or any other host connected to the device.

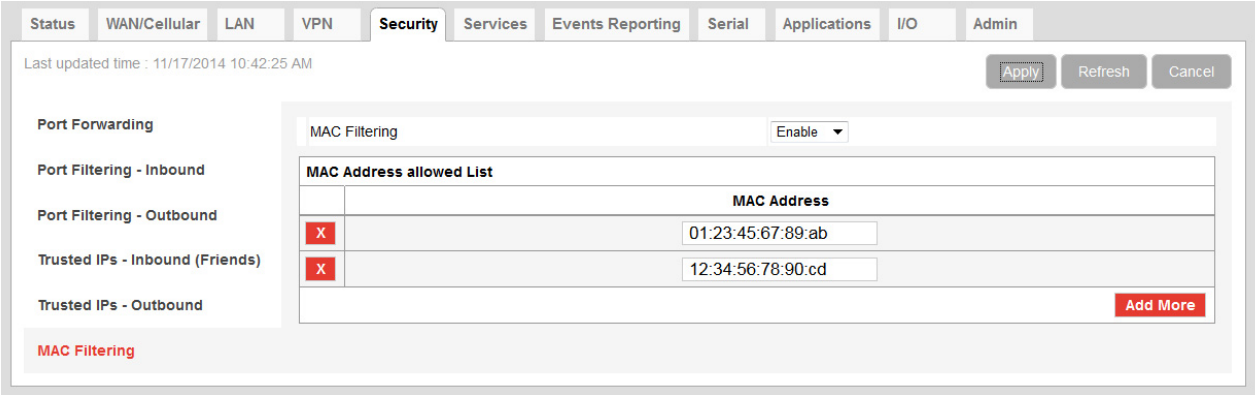


Figure 7-12: ACEmanager: Security > MAC Filtering

Field	Description
MAC Filtering	Enable or disable (default) MAC Filtering
MAC Address allowed List	Allows devices with the MAC Addresses listed to connect to the host and transfer data. Add MAC addresses by clicking on the Add More button. When adding MAC addresses, use a colon between the digit groups, for example 01:23:45:67:89:ab. *Note: After adding all the desired MAC addresses, reboot the device. The MAC Address allowed List takes effect after the device is rebooted.*
MAC Address	This is the MAC Address of the interface adapter on a computer or other device. **Tip:** *You can use the Status > LAN page to obtain the MAC addresses of DHCP connected hosts.*

8: Services Configuration

The pages under the Services tab allow the configuration of external services that extend the functionality of the AirLink Device.

AVMS (AirVantage Management Service)

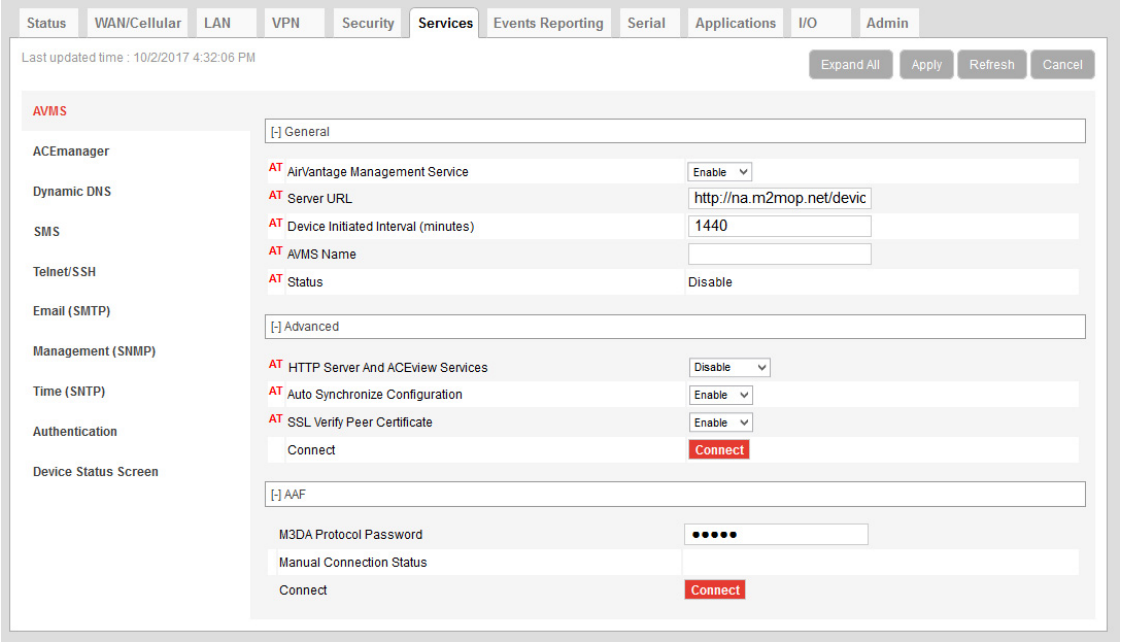


Figure 8-1: ACEmanager: Services > AVMS

Field	Description
General	
AirVantage Management Service	Disables or enables AVMS management by disabling or enabling periodic device-initiated communication with the AVMS server.
Server URL	The AVMS server URL address. By default, this is: http://na.m2mop.net/device/msci/com If you want network traffic from ALEOS to AVMS to be encrypted, enter an HTTPS URL (for example, https://na.m2mop.net/device/msci/com) in this field. Using an HTTPS URL enables Secure Socket Layer (SSL). If SSL is enabled and the SSL Verify Peer Certificate field is set to Enable, the validity of the server certificate is checked. For more information, see SSL Verify Peer Certificate on page 140. *Note: The URL from earlier ALEOS versions, http://na.m2mop.net/device/msci, is still valid. If your AirLink devices are using that URL, there is not need to update it.*

Field	Description
Device Initiated Interval (minutes)	This field determines how often the AirLink device checks for software updates and settings changes from AVMS. AVMS can also query the AirLink device at a regular interval if settings allow. Refer to AirVantage Management Service documentation for more information. Default: 1440 minutes (24 hours).
AVMS Name	Use this field to assign a name of your choice to the AirLink device.This name is used by the AVMS server to identify your device. By default, this field is blank. You can also use an AT command to assign or query the name. See *AVMS_NAME on page 305.
Status	Displays the status of the AVMS connection: • Success — Device successfully contacted AVMS during its latest communication. • Disable — AVMS communications are disabled. (Appears when the AirVantage Management Service drop-down menu is set to Disable.) • [ALEOS] Waiting for connectivity — This transitory status appears when the device is in Connect-on-traffic mode and is trying to connect to the network for an AVMS check-in. (See Always on connection on page 57.) When the device connects to the network, the AVMS check-in is sent and the status changes to Success or an error message, if there is a problem with the connection. For a list of error messages, see page 338.
Advanced	
HTTP Server And ACEview Services	Allows you to activate the: • MSCI server—enables you to configure the gateway remotely using MSCI over HTTP • ACEview service—enables the gateway to communicate with the ACEview Windows utility Options are: • Disable—Both services are disabled. • LAN Only—The MSCI HTTP server and ACEview service are only accessible through a LAN connection. • Both WAN And LAN—The MSCI HTTP server and ACEview service are accessible through both WAN and LAN connections. *Note: In order to use MSCI server-initiated communication from AVMS, HTTP Server And ACEview Services must be set to Both WAN And LAN.*
Auto Synchronize Configuration	This field allows you to choose when changes to the configuration are propagated to AVMS. • Enable—Changes to the configuration are propagated as soon as possible and do not wait for the next communication period (as configured in the Device Initiated Interval field). This may result in more frequent communication with AVMS. (default) • Disable—Changes to the configuration are propagated to AVMS at the device initiated interval rate.

Field	Description
SSL Verify Peer Certificate	This field has no effect unless an HTTPS URL is used for the Server URL. Using an HTTPS URL (for example, https://na.m2mop.net/device/msci/com) as the server URL enables Secure Socket Layer (SSL). When SSL is enabled, use this field to set the SSL certificate validation. • Enable—The validity of the server certificate is checked during the SSL negotiation. (default) If the certificate is not valid, communication with the AVMS server is terminated. For more information, see [HTTP] SSL peer certificate or SSH remote key was not OK on page 339. • Disable—The validity of the server certificate is not checked during the SSL negotiation. The SSL communication proceeds even if the server presents a non-validated certificate.
Connect	The Connect button enables you to manually connect an AirLink device to AVMS. This may be useful for troubleshooting the connection between the platform and the remote device and confirming that AAF scripts or jobs created are executing as expected on AVMS.
Manual Connection Status	Displays the current manual connection status.
Connect	The Connect button enables you to manually connect an AirLink device to AVMS. This may be useful for troubleshooting the connection between the platform and the remote device and confirming that AAF scripts or jobs created are executing as expected on AVMS.

ACEmanager

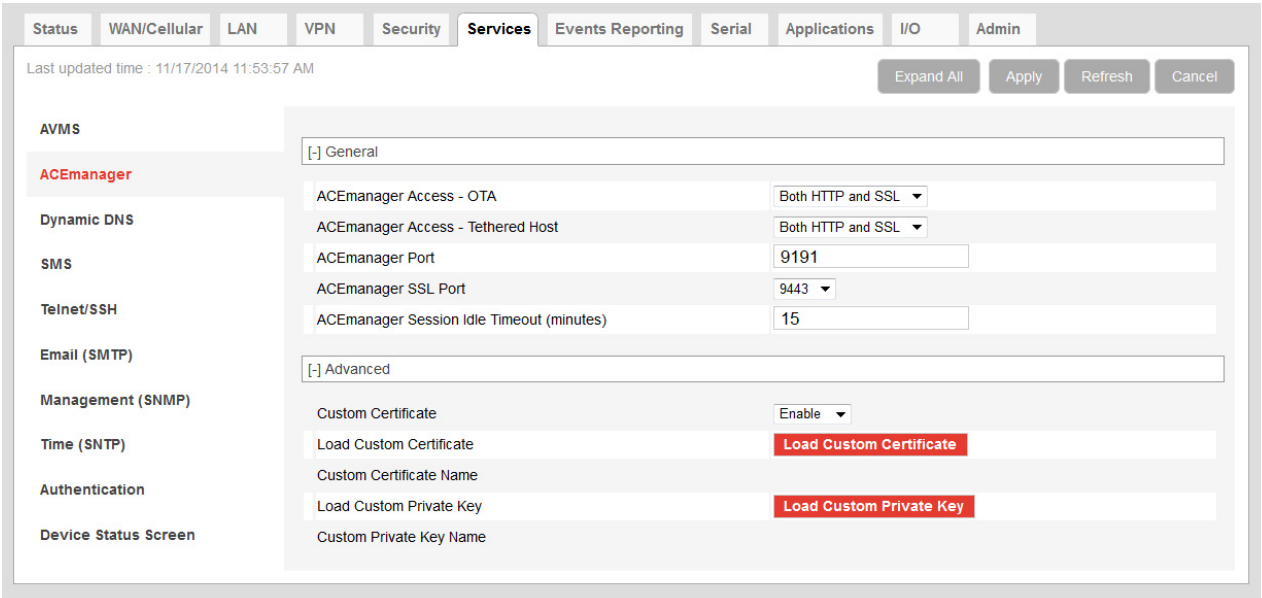


Figure 8-2: ACEmanager: Services > ACEmanager

Field	Description
General	
ACEmanager Access - OTA	Configures over-the-air ACEmanager access. Options are: • Disable (default) • SSL Only • Both HTTP and SSL
ACEmanager Access - Tethered Host	Configures ACEmanager access if tethered (physically connected) to Ethernet, USB, or RS232. Options are: • SSL Only • Both HTTP and SSL (default)
ACEmanager Port	Identifies the port set for ACEmanager. Reboot the device after applying the port change.
ACEmanager SSL Port	Identifies the SSL port set for ACEmanager access. Reboot the device after applying the port change. Options are: • 9443 through 9449 and 443. Default: 9443
ACEmanager Session Idle Timeout (minutes)	If ACEmanager is idle for the configured timeout, it automatically logs out and returns you to the login screen. Options are: • 0–60 (minutes) Default is 15. If you set the ACEmanager Session Idle Timeout to zero (0), the session remains active until you manually log out.
Advanced	
Custom Certificate	Enabling this feature allows you to load a custom SSL certificate. (Some restrictions apply; see Note below for details.) Options are: • Enable—Additional fields appear that allow you to load a custom SSL certificate and a custom private key. The ACEmanager web server uses this custom certificate for authentication during HTTPS communication, instead of the default certificate. • Disable—The ACEmanager web server uses the default SSL certificate for authentication during HTTPS communication. (default) *Note: The custom certificate and private key must meet the following conditions:* • *The certificate must be an X.509 certificate* • *The certificate and the private key must be in .pem format, and they must be in separate files.* • *The encryption cipher suite used must be 128 bits.* • *There is no limit to the size of the private key, but the larger the key, the more the performance is affected. Sierra Wireless recommends that the key does not exceed 2048 bits.*

Field	Description
Load Custom Certificate	This field only appears when the Custom Certificate field is set to Enable. To load a custom SSL certificate: 1. Click Load Custom Certificate. 2. Click Browse... and navigate to the SSL certificate file. 3. Click Upload file to device. 4. Once you have uploaded the custom certificate and the custom private key, click Apply and reboot the device.
Custom Certificate Name	This field only appears when the Custom Certificate field is set to Enable. Displays the name of the custom certificate.
Load Custom Private Key	This field only appears when the Custom Certificate field is set to Enable. Allows you to enter a custom private key (Some restrictions apply; see Custom Certificate on page 141 for details.) To load a custom private key: 1. Click Load Private Key. 2. Click Browse... and navigate to the private key file. 3. Click Upload file to device. 4. Once you have uploaded the custom certificate and the custom private key, click Apply and reboot the device.
Custom Private Key Name	This field only appears when the Custom Certificate field is set to Enable. Displays the name of the private key.

Dynamic DNS

Dynamic DNS allows an AirLink gateway WAN IP address to be published either to a proprietary Sierra Wireless dynamic DNS service called IP Manager, or to an alternate 3rd party Mobile Network Operator.

Whether you have one Sierra Wireless AirLink gateway or multiple devices, it can be difficult to keep track of the current IP addresses especially if the addresses are not static but change every time the devices connect to the mobile network. If you need to connect to a specific gateway, or the device behind it, it is much easier when you have a domain name (mypage.mydomain.com).

Reasons to Contact or Connect to a Device:

- Requesting a location update from a delivery truck
- Contacting a surveillance camera to download logs or survey a specific area
- Triggering an oil derrick to begin pumping
- Sending text to be displayed by a road sign
- Updating the songs to be played on a juke box
- Updating advertisements to be displayed in a cab
- Remote accessing a computer, a PLC, an RTU, or other system
- Monitoring and troubleshooting the status of the device itself without needing to bring it in or go out to it.

A dynamic IP address is suitable for many Internet activities such as web browsing, looking up data on another computer system, for data only being sent out, or for data only being received after an initial request (also called Mobile Originated). However, if you need to contact the AirLink gateway directly, a device connected to the AirLink gateway, or a host system using your AirLink gateway (also called Mobile Terminated), a dynamic IP will not give you a reliable address to contact (since it may have changed since the last time it was assigned).

Domain names are often only connected to static IP addresses because of the way most domain name (DNS) servers are set-up. Dynamic DNS servers require notification of IP Address changes so they can update their DNS records and link a dynamic IP address to the correct name.

- Dynamic IP addresses are granted only when your AirLink gateway is connected and can change each time the gateway reconnects to the network.
- Static IP addresses are granted the same address every time your AirLink gateway is connected and are not in use when your gateway is not connected.

Since many cellular providers, like wire-based ISPs, do not offer static IP addresses or static address accounts (which can cost a premium as opposed to. dynamic accounts), Sierra Wireless AirLink Solutions developed IP Manager. IP Manager works with a Dynamic DNS server to receive notification from Sierra Wireless AirLink gateways to translate the dynamic IP address to a fully qualified domain name. Thus, you can contact your AirLink gateway directly from the Internet using a domain name.

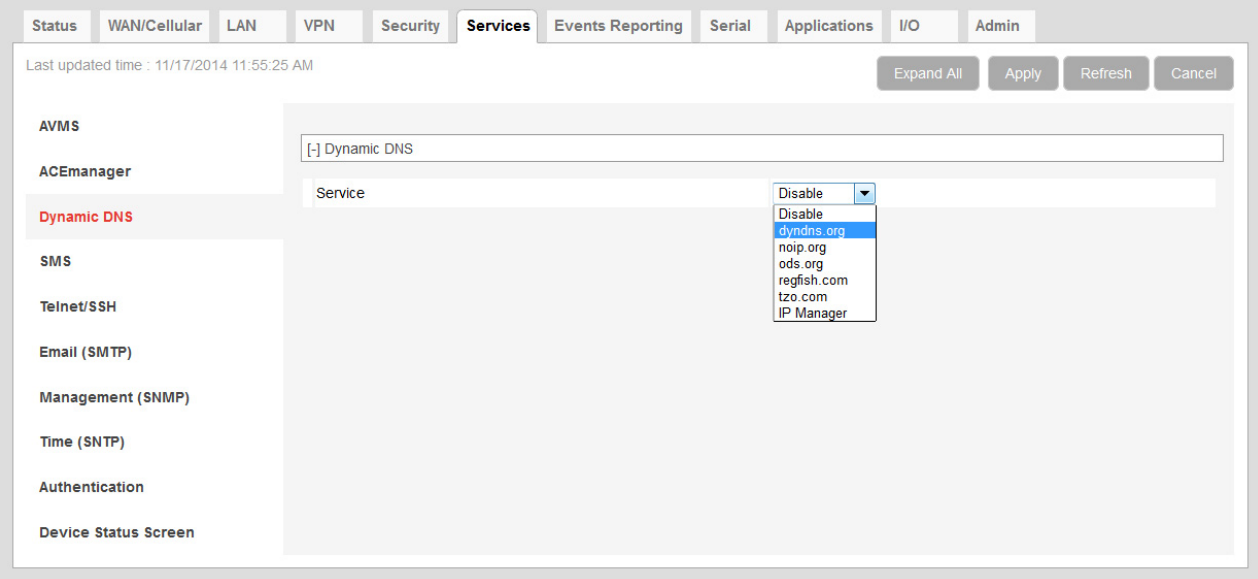


Figure 8-3: ACEmanager: Services > Dynamic DNS Service (partial screen)

Field	Description
Service	Allows you to select a Dynamic DNS Mobile Network Operator. Options are: • Disable (default) • dyndns.org • noip.org • ods.org • regfish.com • tzo.com • IP Manager

3rd party Services

Using a 3rd party dynamic DNS service requires an account with Internet access and an account with the 3rd party service.

Note that 3rd party Dynamic DNS services typically update the domain name to point to the source IP in the update packet. If the gateway has a NATed WAN IP address the domain name points to the network device performing NAT.

Note: Using a Dynamic DNS service does not change the gateway's Internet accessibility. If the gateway cannot be accessed remotely using the WAN IP address, it cannot be accessed using the associated FQDN.

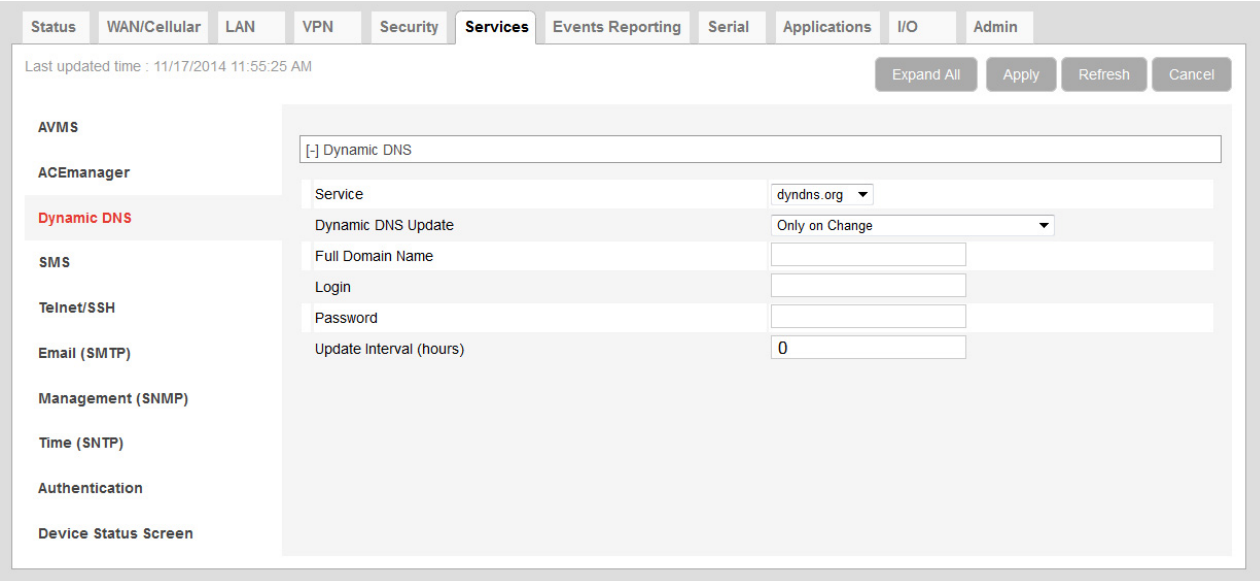


Figure 8-4: ACEmanager: Services > Dynamic DNS 3rd Party Services (partial screen)

Figure 8-4 is a sample 3rd party service information screen. The 3rd party service selected from the Service drop down menu in this example is "dyndns.org." These same fields will be displayed for all Service selections other than IP Manager and Disable.

Field	Description
Service	Allows you to select a Dynamic DNS Mobile Network Operator. Options are: • Disable (default) • dyndns.org • noip.org • ods.org • regfish.com • tzo.com • IP Manager
Dynamic DNS Update	Options are: • Only on Change • Periodically Update (Not Recommended)
Full Domain Name	The name of a specific AirLink gateway or device
Login	Shows the login name
Password	Shows the password in encrypted format
Update Interval (hours)	Indicates the time (in hours) between checks for service updates from the selected 3rd party service when periodic is selected.

IP Manager

You can use the Sierra Wireless IP Manager Dynamic DNS service if:

- The gateway has Internet access and uses the Sierra Wireless-hosted IP Manager server (eairlink.com domain)
- The gateway is on a private network without Internet access and a self-hosted IP Manager server is on the same private network. If you want to self-host an IP Manager server on your private network, contact your authorized Sierra Wireless distributor for more information.

With IP Manager, the gateway's WAN IP is included in the update packet sent to the IP Manager server, so IP Manager always links the gateway's WAN IP address to the domain name configured on the gateway.

Note: Using a Dynamic DNS service does not change the gateway's remote accessibility. If the gateway cannot be accessed remotely using the WAN IP address, it cannot be accessed using the associated FQDN.

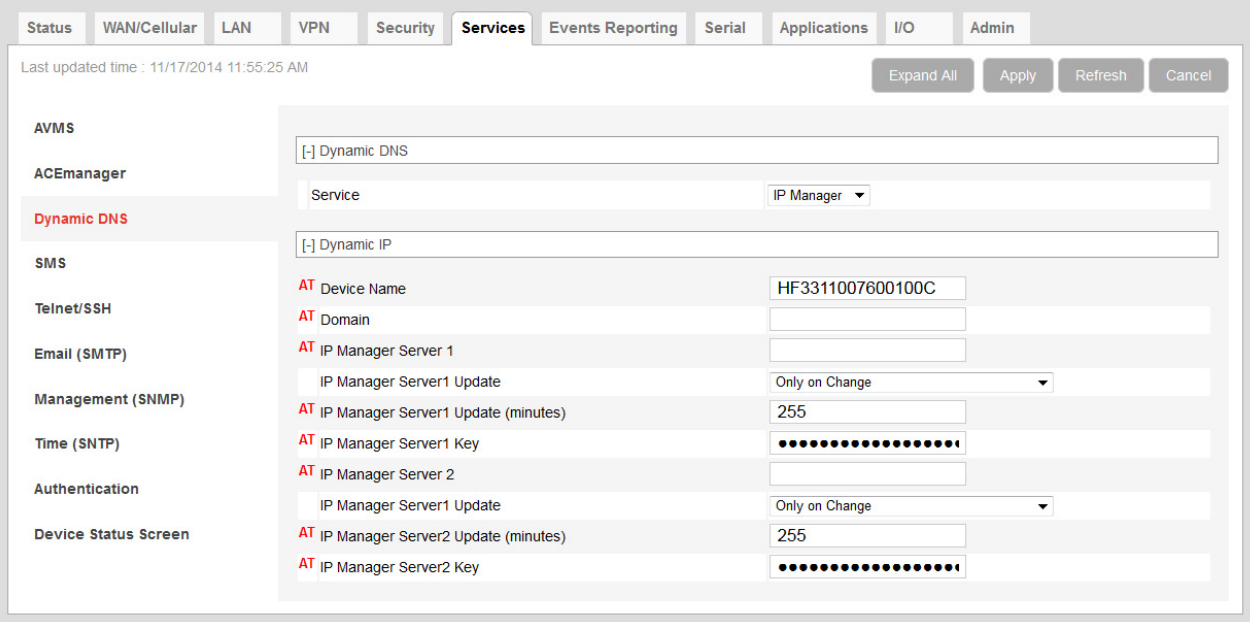


Figure 8-5: ACEmanager: Services > Dynamic DNS IP Manager

Figure 8-5 shows the Dynamic IP fields that appear after selecting IP Manager as your Dynamic DNS Service.

Field	Description
Device Name	The name you want for the device. If you want to use the current device phone number as part of the FQDN (for example, 6175551234.eairlink.com) enter #NETPHONE in this field. #NETPHONE is displayed in this field and everywhere else the device name is used, including on the Home > Status page, in SMS messages, in Event reports, as the PPPoE station name, etc. Using #NETPHONE as the device name is recommended if the account phone number may change and you want the device to continue to use the current phone number as part of the FQDN, or if you are creating a template that will be applied to multiple devices. If you are not using #NETPHONE, the Device Name is limited to alpha-numeric characters, plus – (dash). You cannot include other special characters or spaces. To use this feature, you must have IP Manager selected in the Service field.
Domain	The domain name to be used by the device. This is the domain name of the server configured for *IPMANAGER1. *Note: As a service, Sierra Wireless maintains IP Manager servers that can be used with any AirLink gateway. To use one of the free IP Manager servers, enter eairlink.com in this field.*

Field	Description
IP Manager Server 1 (IP Address) / IP Manager Server 2 (IP Address)	The IP address or domain name of the dynamic DNS server which is running IP Manager. *Note: To use the Sierra Wireless IP Manager server, enter:* *edns1.eairlink.com (IP Manager Server 1)* *edns2.eairlink.com (IP Manager Server 2)*
IP Manager Server 1 Update / IP Manager Server 2 Update	Options are: • Only on Change • Periodic
IP Manager Server1 Update (mins) / IP Manager Server2 Update (mins)	How often, in minutes, you want the address sent to the IP Manager
IP Manager Server 1 Key / IP Manager Server 2 Key	User-defined password key used instead of the AirLink secret key when using an IP Manager server other than the one provided by Sierra Wireless.

Tip: *Some PPPoE connections can use a Service Name to differentiate PPPoE devices. Use the device name to set a Station Name for the PPPoE connection.*

Understanding Domain Names

A domain name is a name of a server or device on the Internet associated with an IP address. Similar to how the street address of your house or your phone number are ways to contact you, both the IP address and the domain name can be used to contact a server or device on the Internet. While contacting you at your house address or with your phone number employ different methods, using a domain name instead of the IP address uses the same method, just as a word based name is easier for most people to remember than a string of numbers.

Understanding the parts of a domain name can help to understand how IP Manager works and what you need to be able to configure the device. A fully qualified domain name (FQDN) generally has several parts.

- **Top Level Domain** (TLD): The TLD is the ending suffix for a domain name (.com, .net, .org, etc.)
- **Country Code Top Level Domain** (ccTLD): This suffix is often used after the TLD for most countries except the US (.ca, .uk, .au, etc.)
- **Domain name**: This is the name registered with ICANN (Internet Corporation for Assigned Names and Numbers) or the registry for a the country of the ccTLD (i.e., if a domain is part of the .ca TLD, it would be registered with the Canadian domain registry). A name must be registered before it can be used.
- **Sub-domain or server name**: A domain name can have many sub-domain or server names associated with it. Sub-domains need to be registered with the domain, but do

not need to be registered with ICANN or any other registry. It is the responsibility of a domain to keep track of its own subs.

mypage.mydomain.com

- ***.com*** is the TLD
- *mydomain* is the domain (usually noted as mydomain.com since the domain is specific to the TLD)
- *mypage* is the subdomain or server name associated with the device, computer, or device registered with mydomain.com

mypage.mydomain.ca

This would be the same as above, but with the addition of the country code. In this example, the country code (.ca) is for Canada.

Tip: *A URL (Universal Resource Locator) is different from a domain name in that it also provides information on the protocol used by a web browser to contact that address such as* `http://www.sierrawireless.com`. www.sierrawireless.com *is a fully qualified domain name, but http://, the protocol identifier, is what makes the whole thing a URL.*

Dynamic Names

When an IP address is not expected to change, the DNS server can indicate to all queries that the address can be cached and not looked up for a long period of time. Dynamic DNS servers, conversely, have a short caching period for the domain information to prevent other Internet sites or queries from using the old information. Since the IP address of a device with a dynamic account can change frequently, if the old information was used (e.g., with a DNS server which indicates the address can be cached for a long period of time) when the IP address changed, the domain would no longer point to the new and correct IP address of the device.

If your AirLink gateway is configured for Dynamic IP when it first connects to the Internet, it sends an IP change notification to the IP Manager. The IP Manager acknowledges the change and updates the Dynamic DNS server. The new IP address will then be the address for your device's configured name.

When your device IP address has been updated in IP Manager, it can be contacted by name. If the IP address is needed, use the domain name to determine the IP address.

Note: The fully qualified domain name of your AirLink gateway will be a subdomain of the domain used by the IP Manager server.

SMS Overview

AirLink gateways can:

- Receive commands via SMS message and send responses, even when the device does not have a data connection (for example, you can provision a device via SMS without having a data connection)
- Act as an SMS gateway for a device connected to a local interface

Note: To use SMS with your AirLink gateway, you must have an account with SMS enabled.

ACEmanager has four SMS modes. Table 8-1 summarizes the capabilities of each mode.

Table 8-1: SMS Mode Capabilities

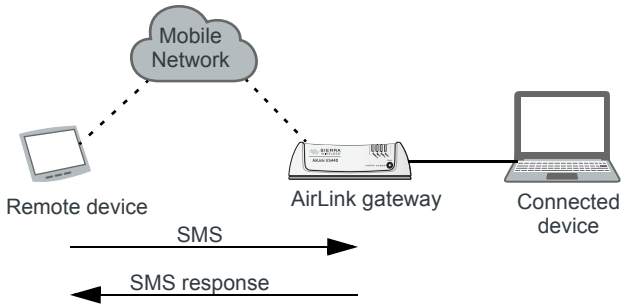
Mode	SMS Command with password	SMS Command without password	SMS Gateway
Password Only	Yes	No	No
Control Only	Yes	Yes*	No
Gateway Only	Yes	No	Yes*
Control & Gateway	Yes	Yes*	Yes*

* Provided either:

- Trusted Phone Number List is disabled.
- Trusted Phone Number List is enabled and the device's phone number is in the Trusted Phone Number List.

For more information on Trusted Phone Number List, see Inbound SMS Messages on page 162.

Sending SMS Commands to an AirLink Gateway



The format for sending an SMS command varies depending on the mode. See Table 8-2 for details.

Table 8-2: SMS Command Formats

Mode	SMS Command Format
Password Only	PW [Password] [Prefix][Command]
Control Only (from a number on the Trusted Phone Number list)	[Prefix][Command] or PW [Password] [Prefix][Command]
Control Only (from a number not on the Trusted Phone Number list)	PW [Password] [Prefix][Command]
Gateway Only	PW [Password] [Prefix][Command]

Note: Insert a space before and after [Password]; no space between [Prefix] and [Command].

Examples:

[Prefix][Command]

"&&&reset", where:

- &&& is the prefix
  If the ALEOS Command Prefix field in ACEmanager (Services > SMS) is blank, the prefix is not required.
- reset is the command

PW [Password] [Prefix][Command]

"PW 1234 &&&reset", where:

- 1234 is the password
  For more information, see SMS Password Security on page 163.
- &&& is the prefix
  If the ALEOS Command Prefix field in ACEmanager (Services > SMS) is blank, the prefix is not required.
- reset is the command

For information on sending SMS commands and a list of available commands, see page 328.

Note: The maximum length of the ALEOS Command Prefix is 3 characters (alphanumeric or special characters).

SMS Modes

The following sections provide instructions for configuring each of these modes and sending SMS messages:

- Password Only
- Control Only

- Gateway Only
- Control and Gateway

For a list of available SMS commands, see page 328. For a list of SMS-related AT commands, see SMS on page 308.

Password Only

In Password Only mode, you can send SMS commands to a device, provided you use the password. Gateway SMS messaging is not supported in this mode.

Note: In Password Only mode, the password is always required. The Trusted Phone Number List is not available.

To configure Password Only mode:

1. In ACEmanager, go to Services > SMS.

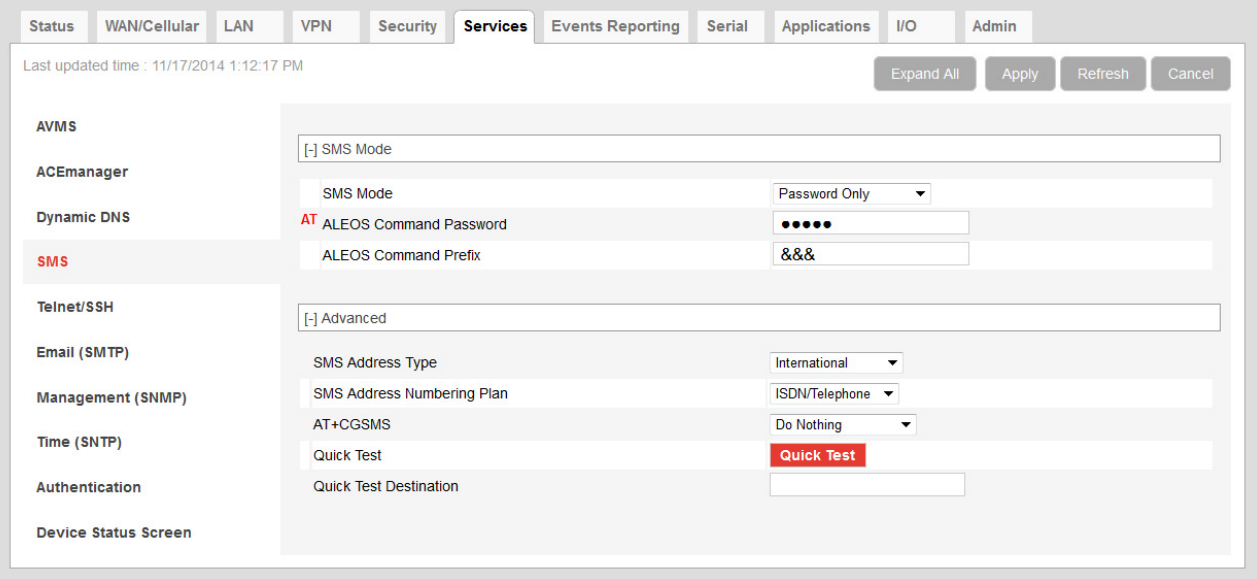


Figure 8-6: ACEmanager: Services > SMS (Password Only)

2. In the SMS Mode field, select Password Only.
3. Enter the desired password in the ALEOS Command Password field or leave the field blank to use the default password.

   The password you enter can be any alphanumeric string between 1 and 255 characters long.

   For more information see SMS Password Security on page 163.
4. If desired, configure SMS Wakeup (see SMS Wakeup on page 160) and Advanced options (see SMS > Advanced on page 165).
5. Click Apply.

For information on the message format, see Sending SMS Commands to an AirLink Gateway on page 149.

Control Only

In Control Only mode, you can send SMS commands to an AirLink gateway, but you cannot send non-command (gateway) SMS messages.

You can send an SMS command without a password if:

- Trusted Phone Number is disabled.
- Trusted Phone Number is enabled and your phone number is on the Trusted Phone Number List.

If Trusted Phone Number is enabled and your number is not on the Trusted Phone Number List, you can still send an SMS command provided you use the password.

Configure ALEOS for Control Only mode

1. In ACEmanager, go to Services > SMS.

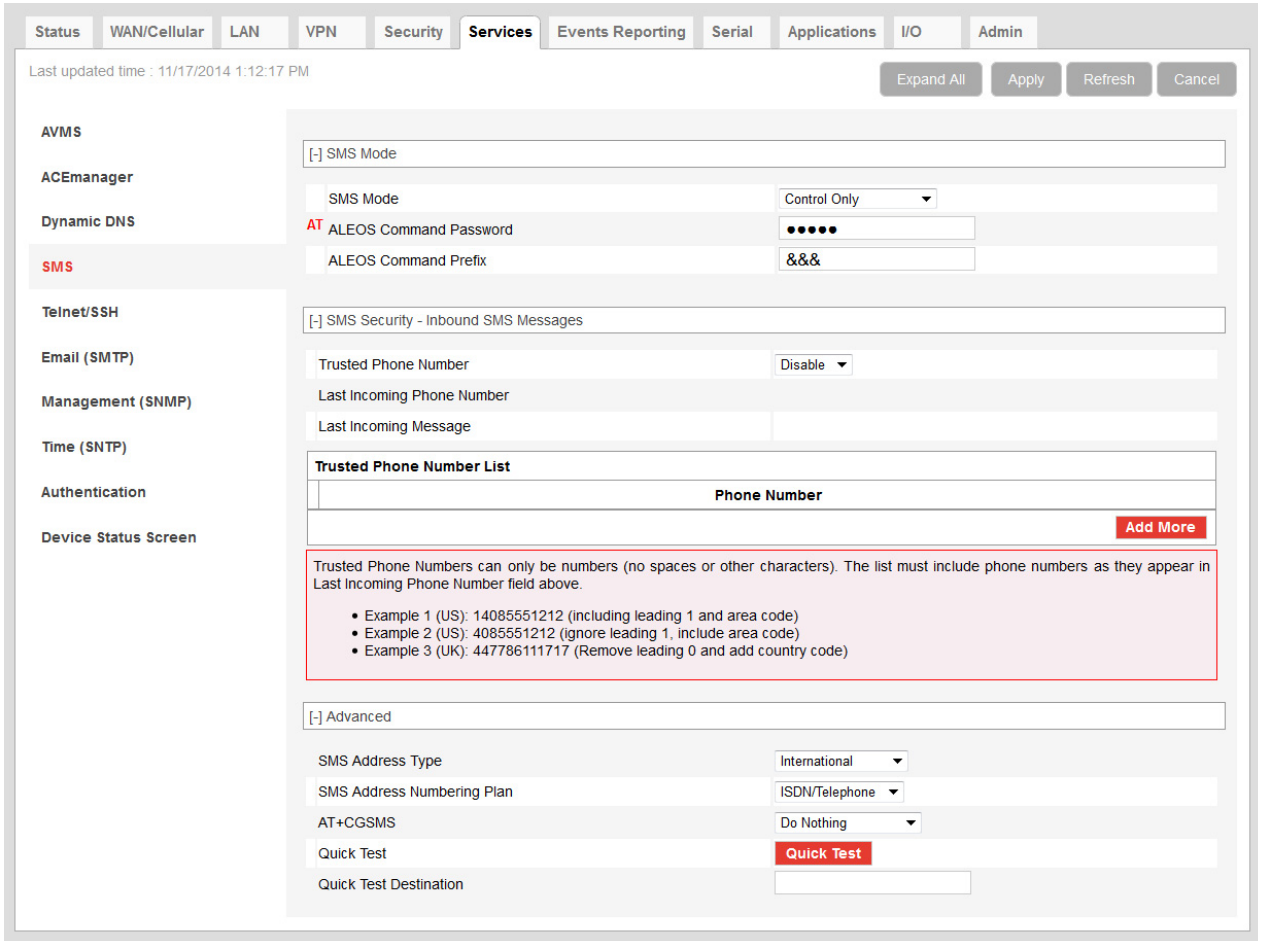


Figure 8-7: ACEmanager: Services > SMS (Control only)

2. In the SMS Mode field, select Control Only.
3. Enter the desired password in the ALEOS Command Password field or leave the field as is to use the default password.

The password you enter can be any alphanumeric string between 1 and 255 characters long.

For more information see SMS Password Security on page 163.

Note: If all the SMS commands you send in Control Only mode are from a trusted number, you do not need to include a password when you send the command.

4. If desired, change the ALEOS Command Prefix or use the default prefix, &&&.

Note: The maximum length of the ALEOS Command Prefix is 3 characters (alphanumeric or special characters). If you leave the ALEOS Command Prefix field blank, no prefix is required when you send the SMS command. The option to omit the prefix is only available in Control Only mode.

5. If desired, configure SMS Security options (see SMS Security on page 162), SMS Wakeup (see SMS Wakeup on page 160), and Advanced options (see SMS > Advanced on page 165).
6. Click Apply.

For information on the message format, see Sending SMS Commands to an AirLink Gateway on page 149.

Gateway Only

In Gateway Only mode you can send and receive SMS gateway messages through the AirLink gateway to a local device. SMS messages received by the AirLink gateway (inbound) are sent on to the configured local device. Messages sent by the local device to a configured port on the AirLink gateway are sent out as SMSs (outbound) to a remote destination. Essentially, the AirLink gateway sends SMS messages between the cellular radio and the connected device.

In Gateway Only mode, you can also send SMS commands provided you include a password. For more information, see Sending SMS Commands to an AirLink Gateway on page 149.

To configure ALEOS for Gateway Only mode and format a Gateway message:

1. In ACEmanager, go to Services > SMS.

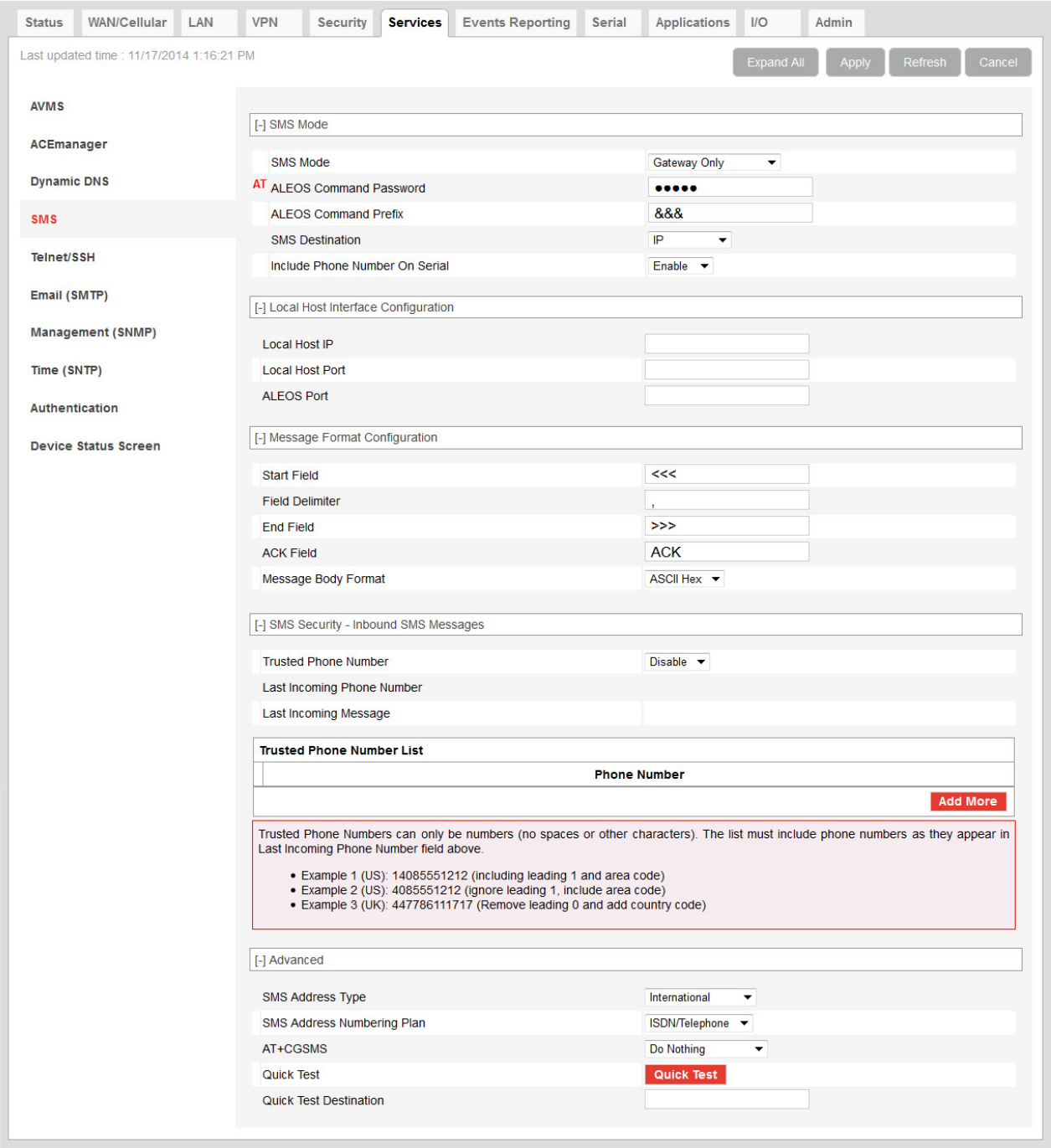


Figure 8-8: ACEmanager: Services > SMS (Gateway Only)

2. In the SMS Mode field, select Gateway Only.
3. Enter the desired password in the ALEOS Command Password field or leave the field blank to use the default password.

   The password you configure can be any alphanumeric string between 1 and 255 characters long.

   For more information see SMS Password Security on page 163.

4. The SMS destination is the local interface where ALEOS forwards an SMS from the mobile network.
   In the SMS destination field, select from the following options:
   - Serial—Messages are forwarded to the Serial port on the destination device.

     If you want to include the phone number as part of the information sent to the serial port, select Yes in the Include Phone Number on Serial field.

     Proceed to step 13.
   - IP—Messages are sent using UDP over IP to a designated LAN device. Proceed to step 5.

Local Device Interface Configuration (Applies to inbound [to the local device] gateway messages when IP is the SMS destination and outbound [from the local device])

Inbound

5. Enter the Local Host IP address.

   This is the IP address of the LAN device that is used as the destination for all incoming Gateway messages.
6. Enter the Local Host Port.

   This is the UDP port the destination device listens to for incoming messages.

Outbound

7. Enter the ALEOS port.

   This is the UDP port on which the AirLink gateway listens for outbound Gateway messages sent from any local device.

Message Format Configuration (Only applies if you selected IP in the SMS destination field)

8. In the Start field, enter the start of message delimiter, or use the default (<<<).
9. In the Field Delimiter field, enter the delimiter to be used between fields in the SMS message, or use the default (,).
10. In the End field, enter the end of message delimiter, or use the default (>>>).
11. In the ACK field, enter the desired acknowledgment message, or use the default (ACK). The acknowledgment is sent to the device as a UDP packet on the same port as the device used to send the message.

    ALEOS provides a message acknowledgment for every SMS message when it is passed to the radio. If ALEOS does not send an ACK, wait for 30 seconds, and then retry.

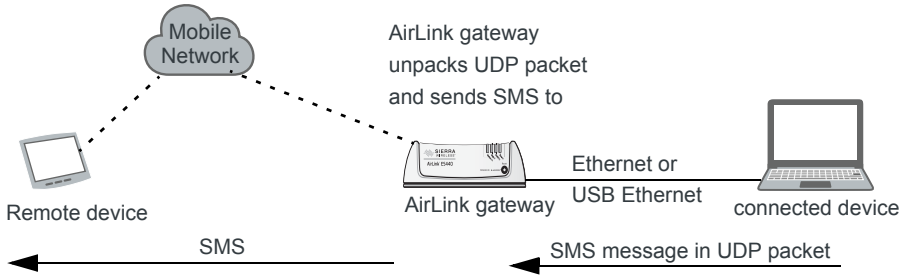
Security

12. If desired, configure SMS Security options (see SMS Security on page 162), SMS Wakeup (see SMS Wakeup on page 160), and Advanced options (see SMS > Advanced on page 165).
13. Click Apply.

    If you are using IP as the destination and you have changed the IPs or port numbers, reboot the device.

For information on the message format for an SMS Command, see Sending SMS Commands to an AirLink Gateway on page 149.

Sending a gateway message from a local IP device to a remote destination



The AirLink gateway acts as a gateway to send SMS messages from an IP connected device using AirLink SMS Protocol. The IP device sends a UDP packet to the AirLink gateway, which then sends the SMS to its destination.

Note: Outgoing SMS messages are limited to 140 characters.

To use AirLink SMS Protocol to send an SMS message from a connected device:

1. Begin with the start field.
2. Follow with the destination phone number. This number must be in the same format as the phone numbers in the Trusted Phone Number List.

Note: There is no space between the start number and the destination phone number or between any delimiter and the data fields.

3. Add the field delimiter.
4. Add the data type for the message:

For:	Enter:
ASCII	ASCII
8-bit	8BIT
Unicode	UCS-2
Data types are case sensitive.	

5. Add another field delimiter.
6. Add the number of ASCII characters in your original message (before it is converted to ASCII hex format).
7. Add another field delimiter.
8. Add the message to be sent in ASCII hex format. ASCII is case sensitive. Do not use any punctuation, such as a colon, or characters between hex pairs.
9. Finish with the end field.

Example: You want to send the following message: “Test message” to phone number (510) 555-4200. To use this feature, convert the message to hex:54657374206d657373616765. Then format the message as follows:

<<<15105554200,ASCII,12,54657374206d657373616765>>>

where:

- “<<<” is the start delimiter
- “15105554200” is the phone number
- “,” is the delimiter between fields
- “ASCII” is the data type
- “12” is the number of characters in the original message (before it is converted to ASCII hex format)
- “54657374206d657373616765” is the message itself
- “>>>” is the end delimiter

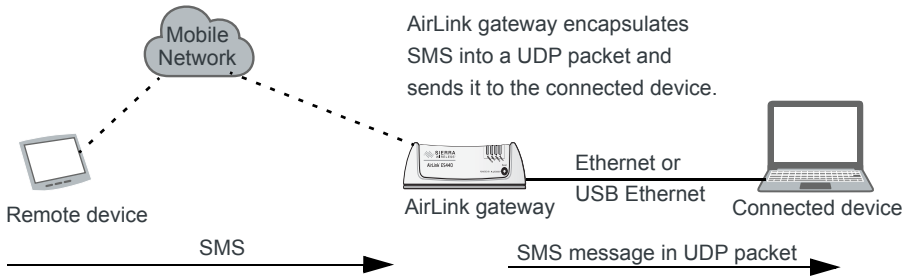
10. Send the UDP packet to the configured ALEOS port.

    After your message is sent, you receive an ACK message in the format ACK Field acknowledgment Code ACK Field. For example, if your message was successfully queued to be sent, you receive the message: ACK0ACK.

If you receive an error message, see SMS on page 332 for details.

*Note: You can also use AT*SMSM2M to send an SMS message to the remote device. For more information, see SMSM2M on page 166.*

Sending a gateway message to the connected device using IP address and port as the SMS destination



Messages from a remote device can be sent to the AirLink gateway. The AirLink gateway encapsulates the message in a UDP packet using AirLink SMS Protocol, and sends it to the configured Local Host IP and Local Host Port on the connected device.

Message example:

Example:

1. An SMS is sent from phone number (640) 555-4200 to the device: “Test message”
2. The AirLink gateway receives the SMS and determines it is a gateway message.
3. The AirLink gateway converts the message into a UDP packet using the AirLink SMS Protocol and sends it to the configured Local Host IP at Local Host Port. The message as follows:

   <<<16045554200,ASCII,12,54657374206d657373616765>>>

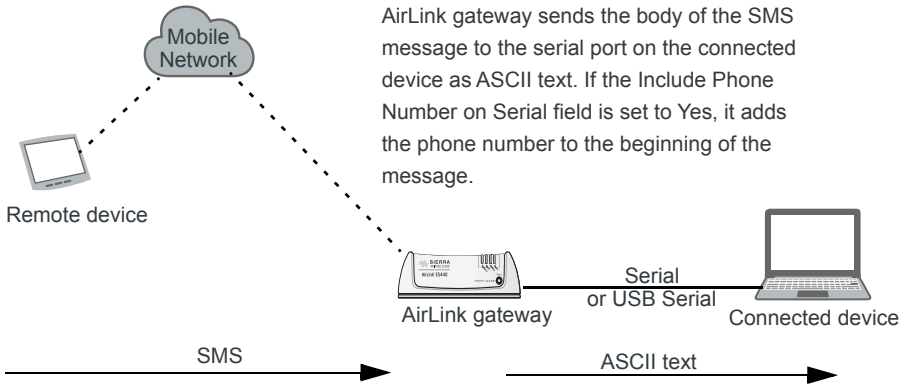
where:

- “<<<” is the start delimiter
- “16045554200” is the phone number
- “,” is the delimiter between fields
- “ASCII” is the message type*
- “12” is the number of characters in the message
- “54657374206d657373616765” is the message itself
- “>>>” is the end delimiter

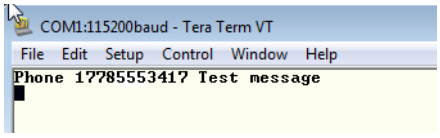
* In this example the message is in ASCII, but it could also be in 8-bit or Unicode format:

For:	Enter:
ASCII	ASCII
8-bit	8BIT
Unicode	UCS-2
Data types are case sensitive.	

Sending a gateway message to the connected device using Serial or USB Serial as the SMS destination



A message can be sent from a remote device to the AirLink gateway. The AirLink gateway sends the body of the message in ASCII text to the connected device. If the Include Phone Number on Serial field is set to Yes, the AirLink gateway prepends the phone number to the message.



Control and Gateway

In Control and Gateway mode you can do both—send commands to the device and send gateway messages to the connected device. When the Trusted Phone Number List is enabled, all SMS messages from trusted devices that do not begin with the password indicator (PW) or the command prefix are sent to the connected device as a gateway message.

For more information, see Trusted Phone Number on page 163.

Configure ALEOS for Control and Gateway mode

1. In ACEmanager, go to Services > SMS.
2. Select Control and Gateway.

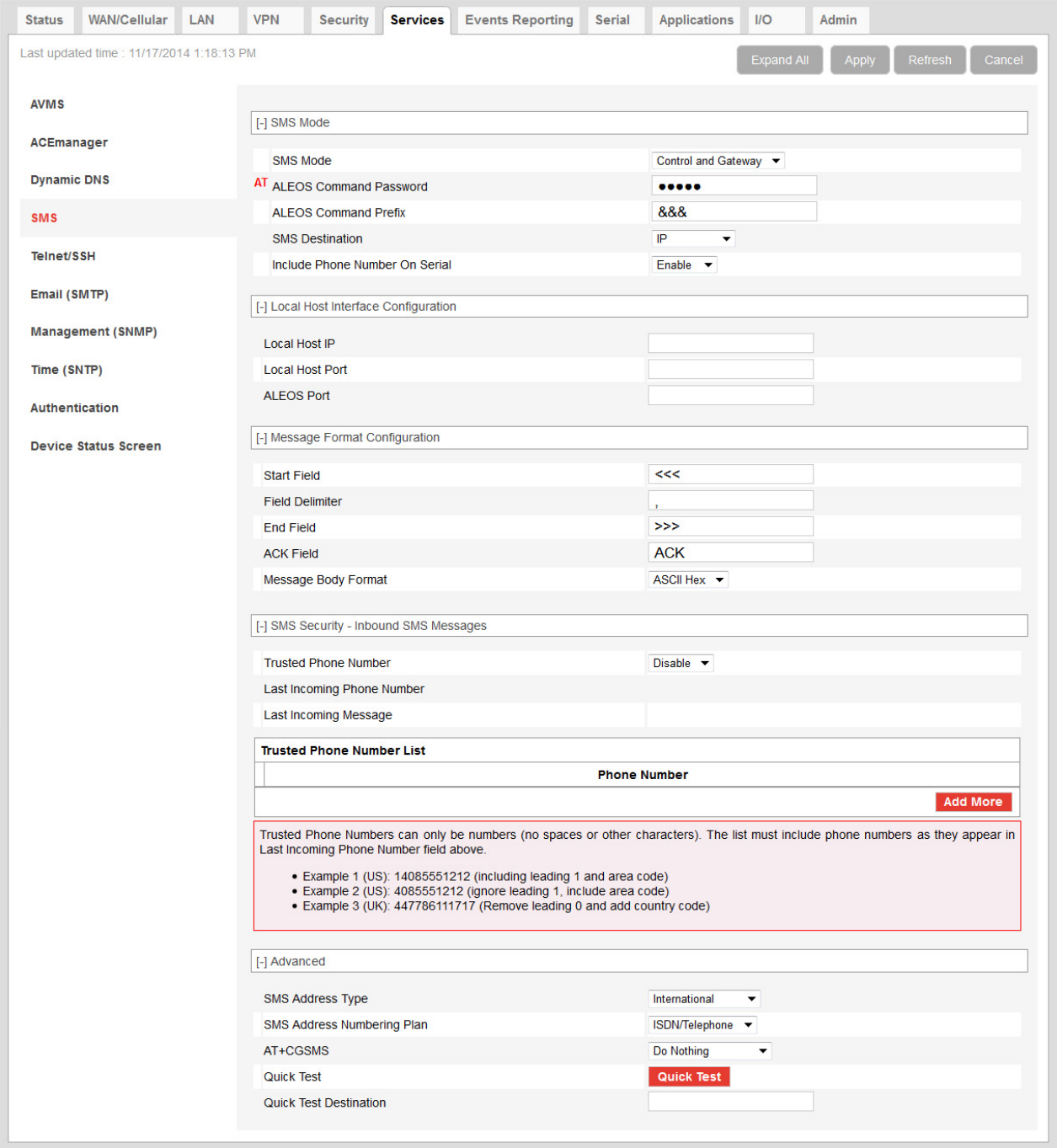


Figure 8-9: ACEmanager: Services > SMS (Control and Gateway)

For more information, see Control Only on page 152 and Gateway Only on page 153.

SMS Wakeup

This feature is supported on International AirLink gateways on the Vodafone network.

When the AirLink gateway is in Connect on traffic mode (for details, see Always on connection on page 57), you can configure the AirLink gateway to also initiate a mobile network data connection on receipt of an SMS. After the connection is established, it remains active until the configured timeout expires. The mobile network data connection closes after the specified timeout period. Outgoing traffic sent after the timer is triggered does not reset the timer.

To configure SMS Wakeup:

1. In ACEmanager go to WAN/Cellular > Advanced and ensure that the Always on connection field is set to Disabled - Connect on traffic.
2. Go to Services > SMS.

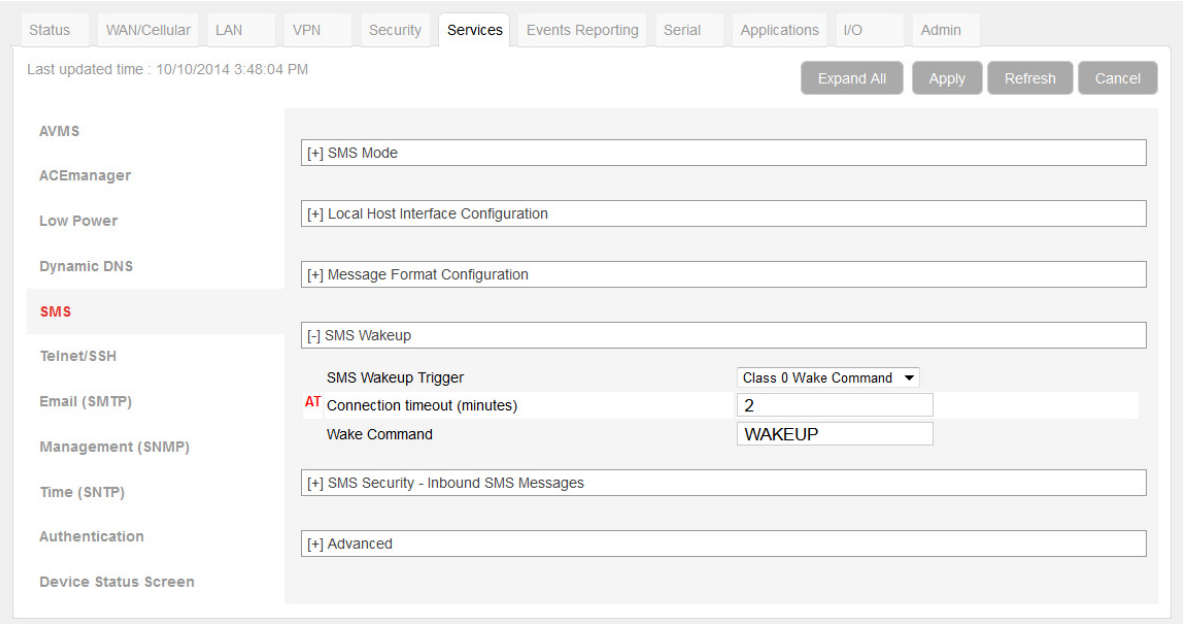


Figure 8-10: ACEmanager: Services > SMS

3. In the SMS Wakeup Trigger field, select the type of SMS that should wake up the device. The options are:
   - Feature Disabled
   - Any Class 0 message
   - Class 0 Wake Command
   - Any SMS message
   - Wake Command

Note: "Class 0 Wake Command" and "Wake Command" are SMS commands.

4. Click Apply.
5. In the Connection timeout (minutes) field, enter the number of minutes the mobile network data connection remains active after SMS Wakeup Trigger is received. Accepted values for this field are 2–65535. The default value is 2.

   You can also set the Connection timeout using an AT command. For more information, see *SMSWUPTOUT on page 309.

6. If you selected Class 0 Wake Command or Wake Command in step 3, you can specify the SMS command name in the Wake Command field or use the default value, WAKEUP. Sending this SMS to the device will wake it up. Example: &&&WAKEUP (&&& is the SMS command prefix.)
7. Click Apply.

SMS Security

Inbound SMS Messages

Incoming SMS messages are received as UDP packets, and forwarded to the local device IP address and port. The UDP packets are in the same format as sent messages.

When Trusted Phone Number security is enabled, incoming messages coming from the phone numbers in the Trusted Phone Number list are the only ones for which commands will be performed (relay, response etc.) or gateway messages forwarded. Incoming messages from all other phone numbers will be ignored. Commands sent to the device with the correct password are always treated as coming from a trusted number.

All non-alphanumeric characters except a space will be replaced by a dot in ACEmanager.

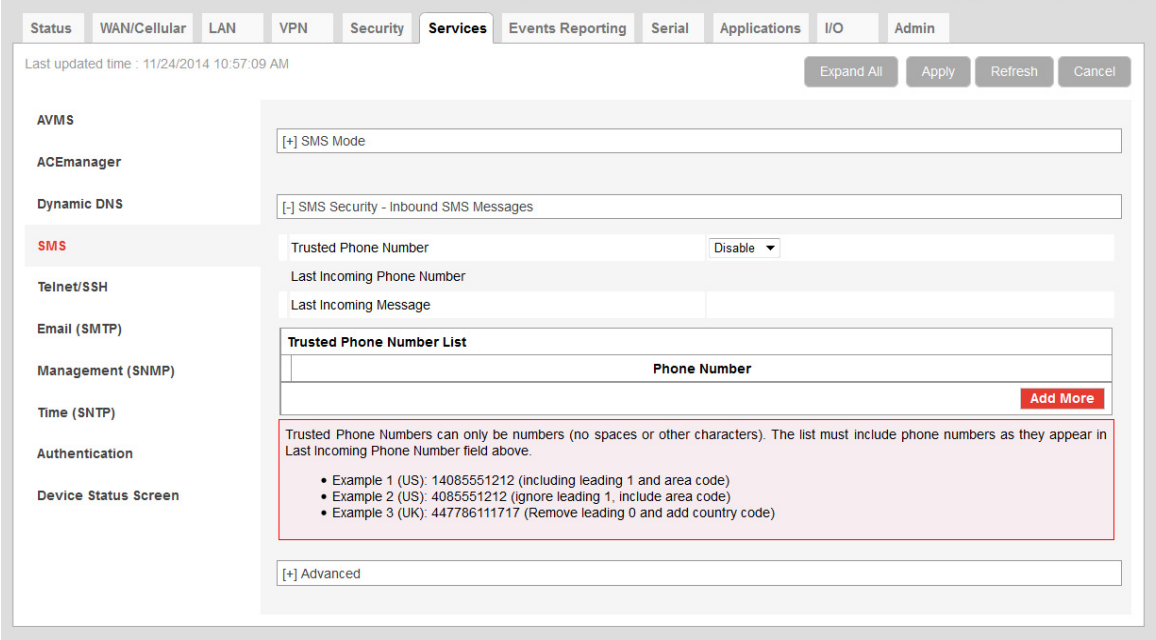


Figure 8-11: ACEmanager: Services > SMS

Field	Description
SMS Security - Inbound SMS Messages	
Trusted Phone Number	Allows you to Enable or Disable a trusted phone number

Field	Description
Last Incoming Phone Number	The last inbound phone number is displayed here. This will only be erased with a reset to defaults.
Last Incoming Message	The last incoming message is the last inbound SMS from the phone number. This will only be erased with a reset to defaults.
Trusted Phone Number List	Trusted phone numbers are listed here

Trusted Phone Number

Follow the instructions below to add a Trusted Phone Number on the SMS page.

1. Send an SMS command to the device, and hit Refresh. If Trusted Phone Number is enabled, and the phone number is not in the Trusted Phone Number List, no action is performed on the message.
2. Once you have the Last Incoming Phone Number that shows up on the SMS window in ACEmanager, note the exact phone number displayed.
3. Click Add More to add the Trusted Phone Number. The Last Phone Number will continue to display. Additions to the Trusted Phone Number become effective immediately. You do not need to reboot the device.

Note: The Trusted Phone number can be up to 15 characters long and must be comprised of numbers only.

Note: Phone Numbers (both trusted and not trusted) will be displayed in the Last Incoming Phone Number field.

4. Enter the Last Incoming Phone Number as the Trusted Phone Number.
5. Click Apply.

Note: Do not enter any extra digits, and use the Last Incoming display as a guide to type the phone number. Use "1" only if it is used in the beginning of the Last Incoming Phone Number.

With Trusted Phone Number enabled, only those SMS messages from Trusted Phone Numbers will receive responses to commands or messages acted on as applicable.

SMS Password Security

The SMS Password feature enables you to use a password to send a command at any time to the device. Even if Trusted Phone Number is enabled, you can send an SMS command from a non-trusted number, provided you include the password.

A default SMS password is generated from the last four characters of the SIM ID (for all SIM-based devices) or the ESN (for devices without a SIM, such those using EV-DO), or you can configure your own SMS password.

Tip: *If you do not know the SIM ID or ESN number you can find it in ACEmanager (Status > WAN/Cellular).*

Note: The SMS password is not the same as the ALEOS password used to access ACEmanager or Telnet/SSH.

To configure the SMS password:

1. Go to Services > SMS > SMS Mode.

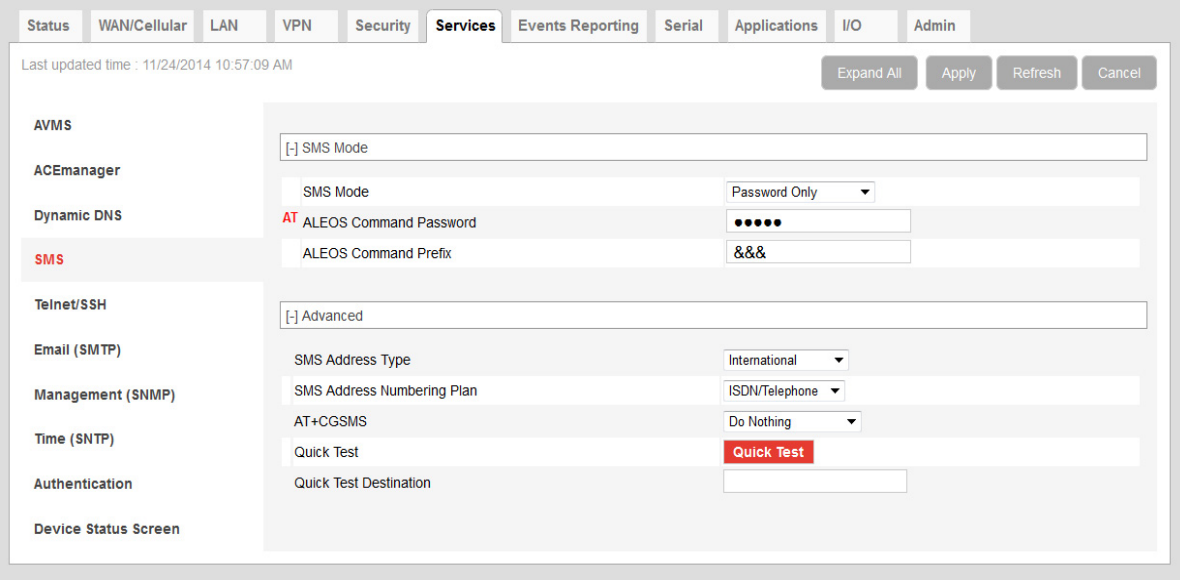


Figure 8-12: ACEmanager: Services >SMS >SMS mode

2. Enter the desired SMS password in the ALEOS Command Password field.

   The password can be any alphanumeric string with a length between 1 and 255 characters.

3. Click Apply.

Note:

- *The SMS password is not displayed in plain text in ACEmanager. If you want to query it, use the AT command. See *SMS_PASSWORD on page 308.*
- *The SMS password is not cleared by a configuration reset.*
- *If an SMS command is sent with the wrong SMS password, the device replies with a "Wrong Password" message, and the command is dropped.*

Using the Default SMS Password

You can use the default SMS password (last 4 characters of either the SIM ID number for SIM-based devices, or the ESN for devices without a SIM) with no prior configuration.

Note: The default password:

- *Works with all SMS commands*
- *Is not displayed in ACEmanager (If the ALEOS Command Password field is blank, the default password is used.)*
- *Is overridden by a user-defined password*
- *Changes if the SIM is changed, if no user-defined password is configured*

SMS > Advanced

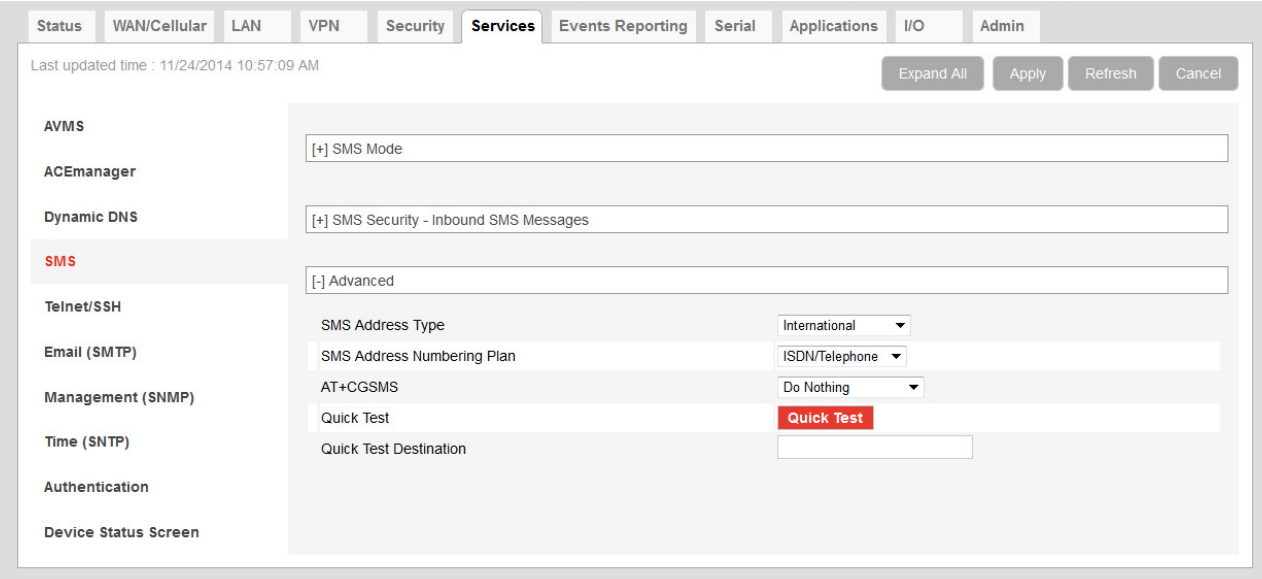


Figure 8-13: ACEmanager: Services > SMS > Advanced

Field	Description
SMS Address Type	For most networks, use the default setting (International). The address type of the phone number used to send outgoing messages and command responses. Options are: • International (default) • National • Network Specific • Subscriber • Abbreviated
SMS Address Numbering Plan	For most networks, use the default setting (ISDN/Telephone). The address numbering plan of the phone number used to send outgoing messages and command responses. Options are: • Unknown • ISDN/Telephone (default) • Date Numbering • Telex • National • Private • ERMES

Field	Description
AT+CGSMS	Allows you to choose the technology used to send SMS messages. For most networks, use the default setting (Do nothing). Options are: • Do nothing (default) • Set AT+CGSMS=0—GPRS • Set AT+CGSMS=1—Circuit switched • Set AT+CGSMS=2—GPRS Preferred (Uses circuit switched if GPRS is not available) • Set AT+CGSMS=3—Circuit Switched Preferred (Uses GPRS if circuit switched is not available) *Note: If your gateway is able to receive SMS messages, but is unable to send them, try changing this field to Set AT+CGSMS=1.* *Note: This field does not appear on CDMA/EV-DO devices or on LTE devices that fallback to CDMA/EV-DO.*
Quick Test	Allows you to send a test message to the destination entered in the Quick Test Destination field.
Quick Test Destination	Enter the phone number to use for the test message. Click Apply before clicking the Quick Test button. This field is cleared on reboot.

SMSM2M

SMS messages can be sent from the serial command interface. Enter AT*SMSM2M=”[phone] [message]”. The phone number needs to be in the same format as numbers entered in the Trusted Phone Number List.

The message must not exceed 140 characters. To send several messages back to back, you must wait for the OK before sending the next message.

Command	Description
***SMSM2M** ***SMSM2M_8** ***SMSM2M_u**	*SMSM2M is the command for ASCII text. *SMSM2M_8 is the command for 8-bit data. *SMSM2M_u is the command for unicode. Format: *smsm2m=”[phone][ascii message]” *smsm2m_8=”[phone][hex message]” *smsm2m_u=”[phone][hex message]” • The phone number can only consist of numbers (NO spaces or other characters). The phone number should be as it appears in the Last Incoming Phone Number field. Example 1 (US): 14085551212 (including leading 1 and area code) Example 2 (US): 4085551212 (ignore leading 1, include area code) Example 3 (UK): 447786111717 (remove leading 0 and add country code) Command Examples: *smsm2m=”18005551212 THIS IS A TEST” sends in ASCII. *smsm2m_8="17604053757 544849532049532041205445535 4" sends the message “THIS IS A TEST” as 8-bit data. *smsm2m_u="17604053757 000102030405060708090a0b0c0d0e0f808182838485868788898A8b8c8d8e8f" sends the bytes: 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f *Note: Not all cellular carriers support 8-bit or unicode SMS messages.*

Telnet/SSH

Use the Telnet or SSH protocol to connect to any AirLink gateway and send AT commands.

A secure mechanism to connect remote clients is a requirement for many users. In ACEmanager, Secure Shell (SSH) is supported to ensure confidentiality of the information and make the communication less susceptible to snooping and man-in-the-middle attacks. SSH also provides for mutual authentication of the data connection.

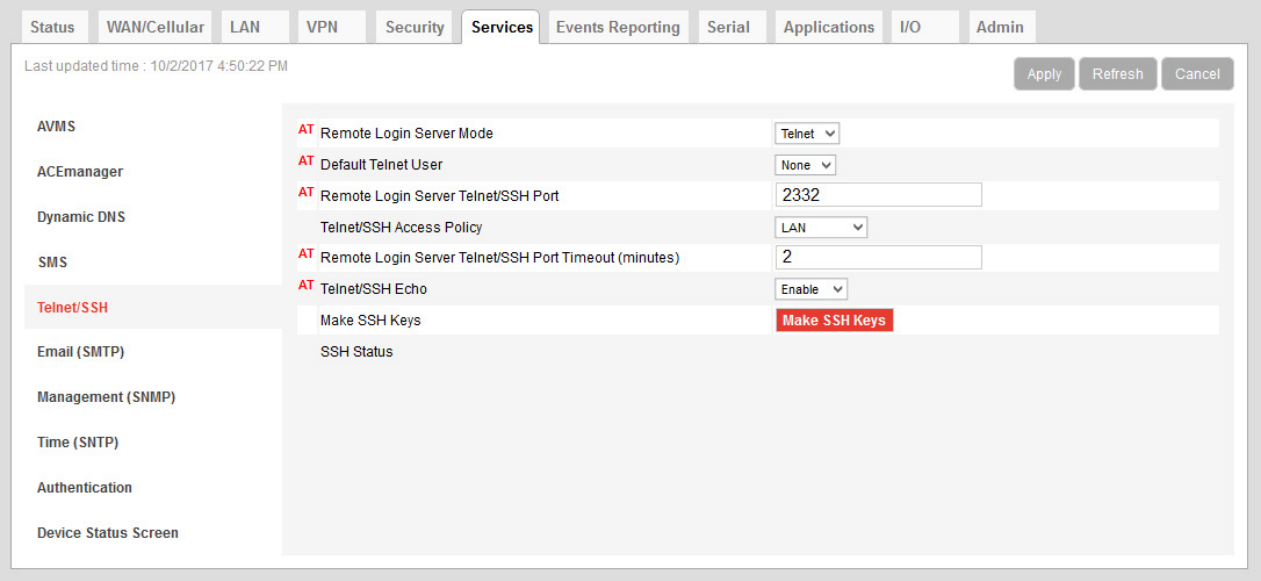


Figure 8-14: ACEmanager: Services >Telnet/SSH

Field	Description
Remote Login Server Mode	Select either Telnet (default) or SSH mode.
Default Telnet User	Select a default Telnet User name Options are: • None—When you log into a Telnet session, you are prompted for a user name and password. • user—When you log into a Telnet session, you are prompted only for a password. Telnet uses the default user name (user). *Note: The default user name is only for Telnet; not SSH.*

Field	Description
Remote Login Server Telnet/SSH Port	Sets or queries the port used for the AT Telnet/SSH server. Default: 2332 **Tip:** *Many networks have the ports below 1024 blocked. We recommend that you use a higher numbered port.*
Telnet/SSH Access Policy	Use this field to restrict access to Telnet/SSH. Options are: • LAN+WAN • LAN (default) • Disabled
Remote Login Server Telnet/SSH Port Timeout (mins)	Telnet/SSH port inactivity time out. Default: 2 (minutes)
Telnet/SSH Echo	Enable (default) or disable AT command echo mode.
Make SSH Keys	Creates keys for SSH session applications
SSH Status	Provides the status of the SSH session

Note: When you are connected to SSH locally, you cannot have OTA SSH connected.

Email (SMTP)

For some functions, the device needs to be able to send email. Since it does not have an embedded email server, you need to specify the settings for a relay server for the device to use.

A reboot is required after configuring the email settings.

Note: The SMTP function will only work with a mail server that will allow relay email from the ALEOS device's Net IP.

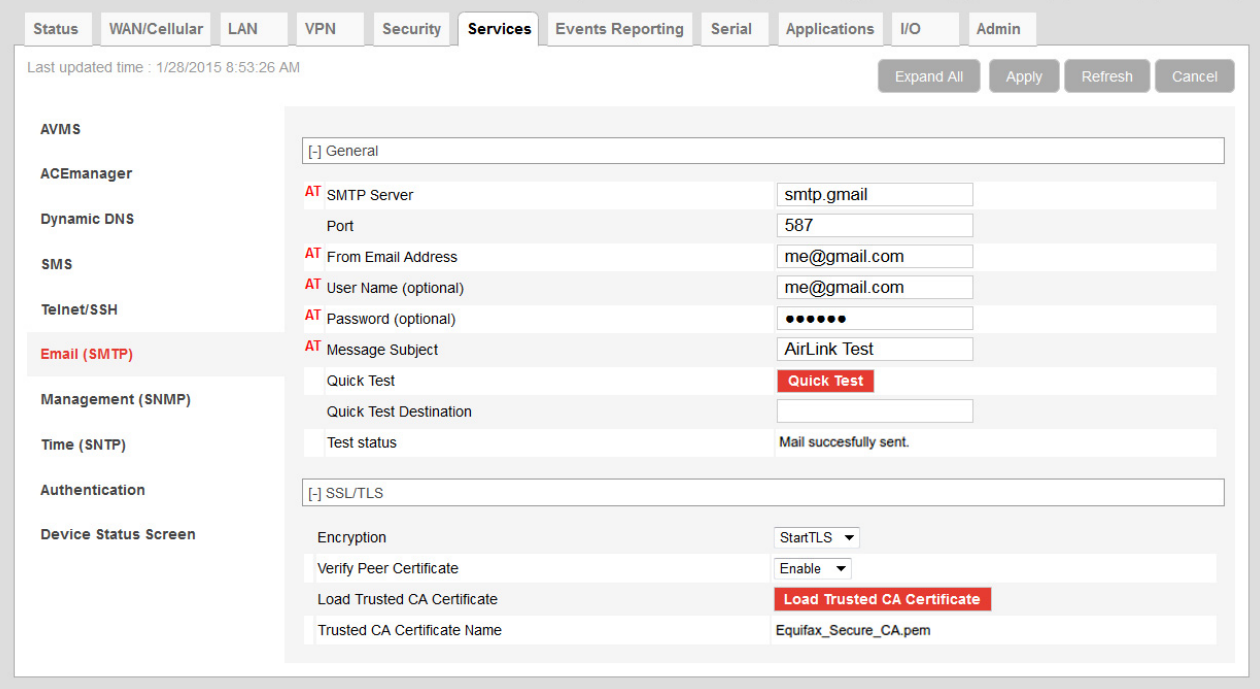
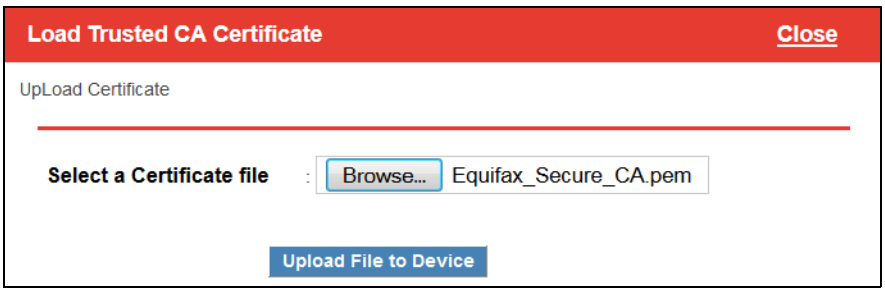


Figure 8-15: ACEmanager: Services > Email (SMTP)

Field	Description
General	
SMTP Server	Specify the IP address or Fully Qualified Domain Name (FQDN) of the SMTP server to use. • d.d.d.d = IP Address • name = domain name (maximum: 40 characters)
Port	Server port (Default is 25.) **Encryption method** / **Default port** SSL / 465 StartTLS / 587
From Email Address	Sets the email address from which the SMTP message is being sent. • email = email address (maximum: 30 characters)
User Name (optional)	Specifies the username to use when authenticating with the server
Password (optional)	Sets the password to use when authenticating the email account (*SMTPFROM) with the server (*SMTPADDR). • pw = password *Note: The email server used for the relay may require a user name or password.*

Field	Description
Message Subject	Allows configuration of the default Subject to use if one is not specified in the message by providing a “Subject: xxx” line as the initial message line. • subject = message subject
Quick Test	After completing the other fields on this screen, click the Quick Test button to send a test email. The status of the test appears in the Test status field.
Quick Test Destination	Enter the email address you want the test email sent to.
Test status	After you press the Quick Test button, the status of the email test appears in this field.
SSL/TLS	
Encryption	Choose the encryption method: • None—No encryption is used (default) • SSL—Use a secure connection directly • StartTLS—Transforms an non-secure connection to a secure one For SSL and StartTLS default ports, see Port on page 170.
Verify Peer Certificate	Choose whether or not to use a peer certificate Disable—No certificate is used (default) Enable—Verifies that the server name used for the connection matches the name and alternative names in the certificate loaded using the Load Trusted CA Certificate field.
Load Trusted CA Certificate	To load a certificate: 1. Click the Load Trusted CA Certificate button. 2. Click browse and navigate to the certificate you want to load.  3. Click Upload File to Device. *Note: Because the starting and expiration dates of the certificate are checked, the date used by the device must be correct. Sierra Wireless strongly recommends that you enable Network Time Protocol (NTP) on the Services > Time (SNTP) tab.*
Trusted CA Certificate Name	The name of the loaded certificate appears in this field.

Management (SNMP)

The Simple Network Management Protocol (SNMP) is designed to allow for remote management and monitoring of a variety of devices from a central location. It is generally used to monitor conditions that may require attention.

The SNMP management system is composed of:

- One or more managers (administrative computers)
- SNMP-compliant devices (such as your AirLink gateway, a router, a UPS, a web server, a file server, or other computer equipment)
- An agent (data collection software running on the SNMP-compliant devices)
- A Network Management System (NMS) that monitors all the agents on a specific network.

The agent stores information about the device in a Management Information Base (MIB). The manager can send messages to this database to configure and query the status of the device. In addition, the agent running on the device can send traps (unsolicited messages) to the manager on startup, on status change, or when an error condition occurs.

AirLink gateways supports SNMPv2c and SNMPv3 and you can configure them as SNMP agents.

Authentication ensures SNMP messages coming from the AirLink gateway have not been modified and the device cannot be queried by unauthorized users. SNMPv3 uses a User-Based Security Model (USM) to authenticate and, if desired or supported, message encryption. USM uses a user name and password specific to each device.

A reboot is required after configuring SNMP.

SNMPv2

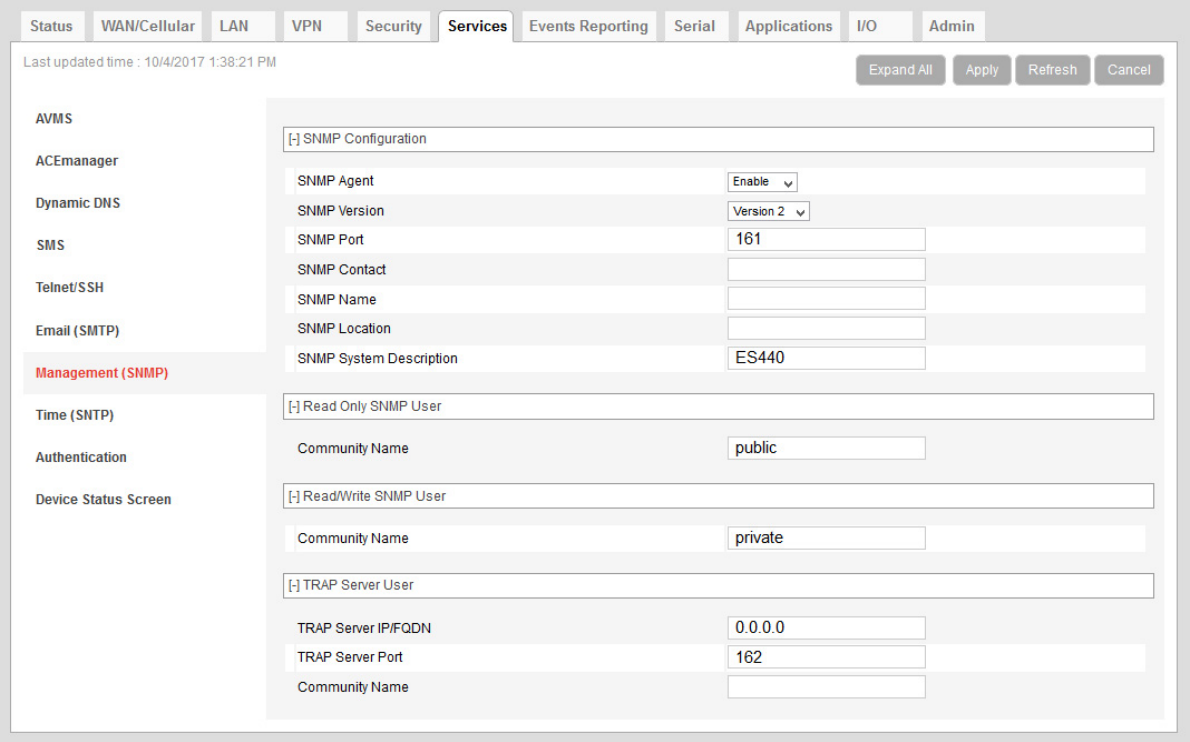


Figure 8-16: ACEmanager: Services> Management (SNMPv2)

Field	Description
SNMP Configuration	
Enable SNMP	Allows you to enable/disable SNMP Default: Disable
SNMP Version	Allows you to select either SNMP protocol Version 2 (default) or Version 3 communications.
SNMP Port	Controls which port the SNMP Agent listens on: • 1–65535 • Default is 161.
SNMP Contact	This is a personal identifier of the contact person you want to address queries to. This is a customer defined field.
SNMP Name	This is the name of the device you want to refer to. This is a customer defined field.
SNMP Location	Location of where your device is stored Enter a meaningful description of where the AirLink gateway is located.
SNMP System Description	Use this field to enter a system description, if desired. The default value, which appears after the SNMP agent is enabled and the gateway rebooted, is the product name.

Field	Description
Read Only SNMP User	
Community Name	The community name is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the device. Default is public.
Read/Write SNMP User	
Community Name	The community name is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the device. Default is private.
TRAP Server User	
TRAP Server IP/FQDN	Identifies the IP address or fully qualified domain name (FQDN) of the trap server that the AirLink gateway sends SNMP traps to
TRAP Server Port	Identifies the specific port the trap server is on • 1–65535 • Default is 162.
Community Name	The community name is a text string that acts as a password. It is used to authenticate messages that are sent between the management station and the device. There is no default value.

SNMPv3

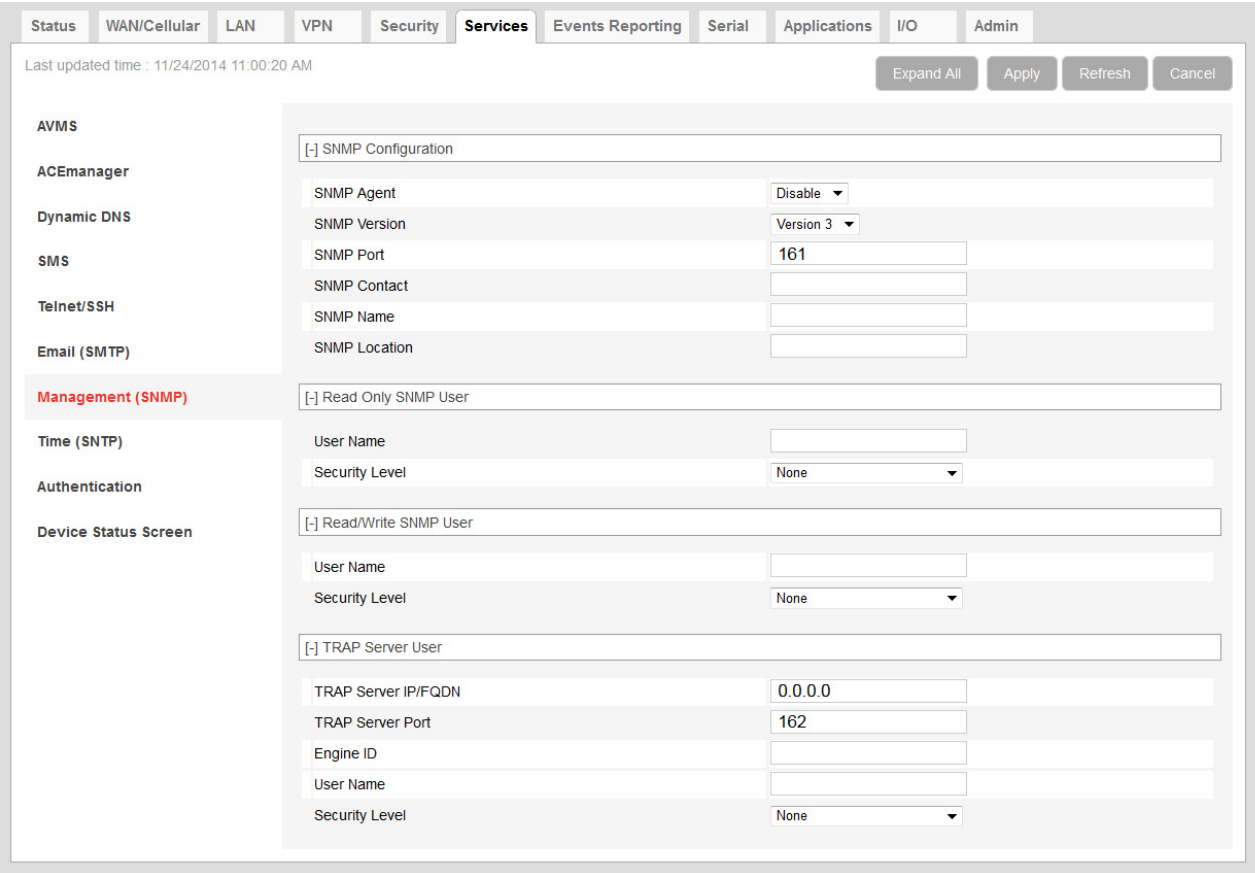


Figure 8-17: ACEmanager: Services> Management (SNMPv3)

Field	Description
SNMP Configuration	
Enable SNMP	Allows you to enable/disable SNMP Default is Disable.
SNMP Version	Allows you to select either SNMP protocol Version 2 (default) or Version 3 communications.
SNMP Port	Controls which port the SNMP Agent listens on: • 1 – 65535 • Default is 161.
SNMP Contact	This is a personal identifier of the contact person you want to address queries to. This is a customer defined field.
SNMP Name	This is the name of the device you want to refer to. This is a customer defined field.
SNMP Location	Location of where your device is stored. This is a customer defined field.

Field	Description
Read Only SNMP	
User Name	Allows these SNMP users to view, but not change the network configuration
Security Level	Security types available: None, Authentication Only, and Authentication and Privacy.
Authentication Type	Authentication types available: MD5 or SHA *Note: This field is only available when you select either Authentication and Privacy, or Authentication Only in the Security Level field.*
Authentication Key	This key authenticates SNMP requests for SNMPv3. • Minimum length: 8 ASCII characters • Maximum length: 255 ASCII characters Example: My Key_1234 *Note: This field is only available when you select either Authentication and Privacy, or Authentication Only in the Security Level field.*
Privacy Type	Privacy types available: AES or DES *Note: This field is only available when you select Authentication and Privacy in the Security Level field.*
Privacy Key	This key ensures the confidentiality of SNMP messages via encryption • Minimum length: 8 ASCII characters • Maximum length: 255 ASCII characters Example: My Key_56789 *Note: This field is only available when you select Authentication and Privacy in the Security Level field.*
Read/Write SNMP For a description of the Read/Write SNMP fields, see Read Only SNMP on page 176.	
TRAP Server User	
TRAP Server IP/FQDN	Identifies the IP address or fully qualified domain name (FQDN) of the trap server that the AirLink gateway sends SNMP traps to
TRAP Server Port	Identifies the specific port the trap server is on • 1 – 65535 • Default is 162.

Field	Description
Engine ID	The Engine ID is a mandatory field that uniquely identifies the SNMPv3 agent in the device to the server. The Engine ID is 5–32 octets long (1 octet is 2 hex characters). That is: • Minimum length: 10 hex characters • Maximum length: 64 hex characters Create the engine ID by entering hex characters only, with no leading 0x. For example, ABCDEF1020
User Name	See User Name on page 176.
Security Level	See Security Level on page 176.
Authentication Type	See Authentication Type on page 176.
Authentication Key	See Authentication Key on page 176.
Privacy Type	See Privacy Type on page 176.
Privacy Key	See Privacy Key on page 177.

Time (SNTP)

The device can be configured to synchronize its internal clock with a time server on the Internet using the Simple Network Time Protocol.

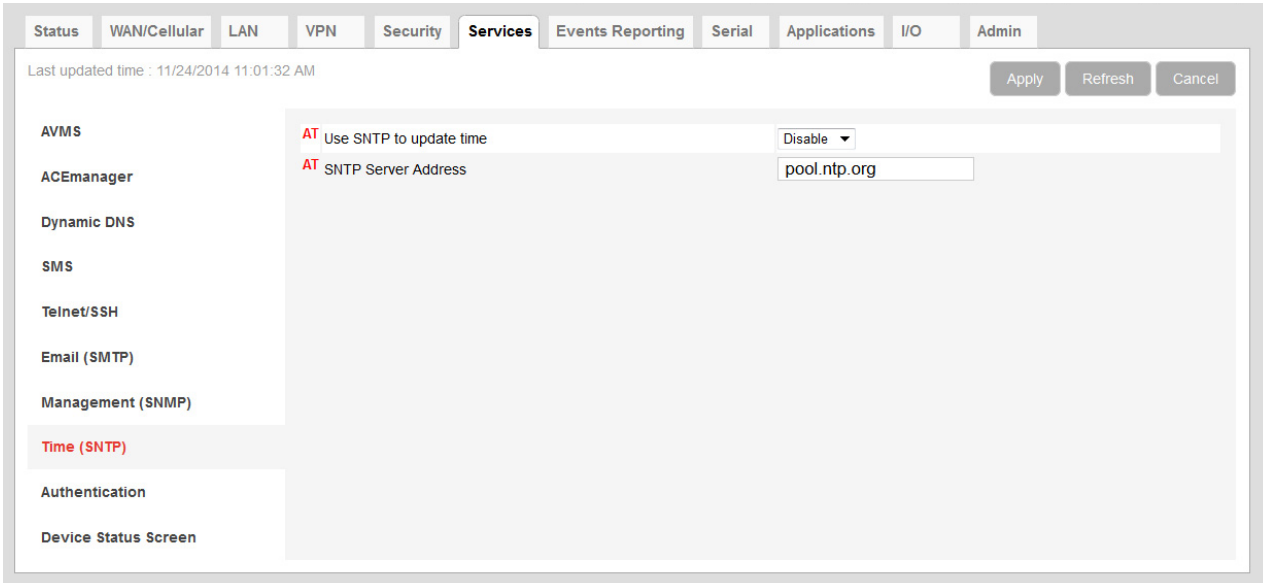


Figure 8-18: ACEmanager: Services > Time (SNTP)

Field	Description
Enable time update	Enables daily SNTP update of the system time. Default: Disable
SNTP Server Address	SNTP Server IP address, or fully qualified domain name, to use if *SNTP=1. If blank, time.nist.gov is used. • d.d.d.d=IP address • name=domain name

Authentication

ALEOS supports ACEmanager login using secure LDAP, RADIUS, and TACACS+ authentication schemes. This enables enterprise IT managers to centrally manage access to AirLink gateways and produce an audit trail showing which users logged into specific devices and when.

Note the following:

- You can configure any or all of these schemes at the same time. When more than one scheme is configured, the authentication is successful if at least one of the schemes authenticates the user.
- Successful authentication can take time. For example, if you have all three authentication schemes enabled, ALEOS first attempts to reach the LDAP server. If it is unable to reach the LDAP server in the configured timeout period, it abandons the attempt and tries to reach the RADIUS server. If that server is unreachable after the timeout period, it then tries to reach the TACACS+ server. If none of the servers are reachable in the configured timeout periods, ALEOS falls back to ACEmanager user name and password authentication.
- LDAP, RADIUS, and TACACS+ provide authentication (checks the user's credentials) but do not check authorization (account expiration date, user rights, etc.) All users authenticated using the LDAP, RADIUS, and TACACS+ servers have administrative rights (i.e. a user account) and can modify the AirLink gateway settings. Ensure that LDAP, RADIUS, and TACACS+ users are authorized to modify device settings.
- LDAP, RADIUS, and TACACS+ are supported for ACEmanager logins, but are not supported by other AirLink gateway services such as Telnet, SSH, PPPoE, etc.

For instructions on configuring these authentication schemes, see:

- LDAP Authentication on page 178
- RADIUS Authentication on page 180
- TACACS+ Authentication on page 181

LDAP Authentication

Lightweight Directory Access Protocol (LDAP) is a network protocol for accessing and manipulating information stored in a directory. It is suitable for using with information that must be easily available and accessible, and does not change frequently. AirLink gateways support LDAP version 3.

To configure LDAP:

1. Go to Services > Authentication.
2. In the LDPA Client field, select Enable.
3. Enter:
   - The LDAP server IP address or resolvable domain name
   - The Port number (default is TCP port 389)
4. Ensure that the LDAP server IP address/port is reachable not only from outside the company, but also from inside the mobile network your gateway is on.

   You can use a utility such as netcat to test this. If netcat is available try:
   nc -z <IP> <port>; echo $?

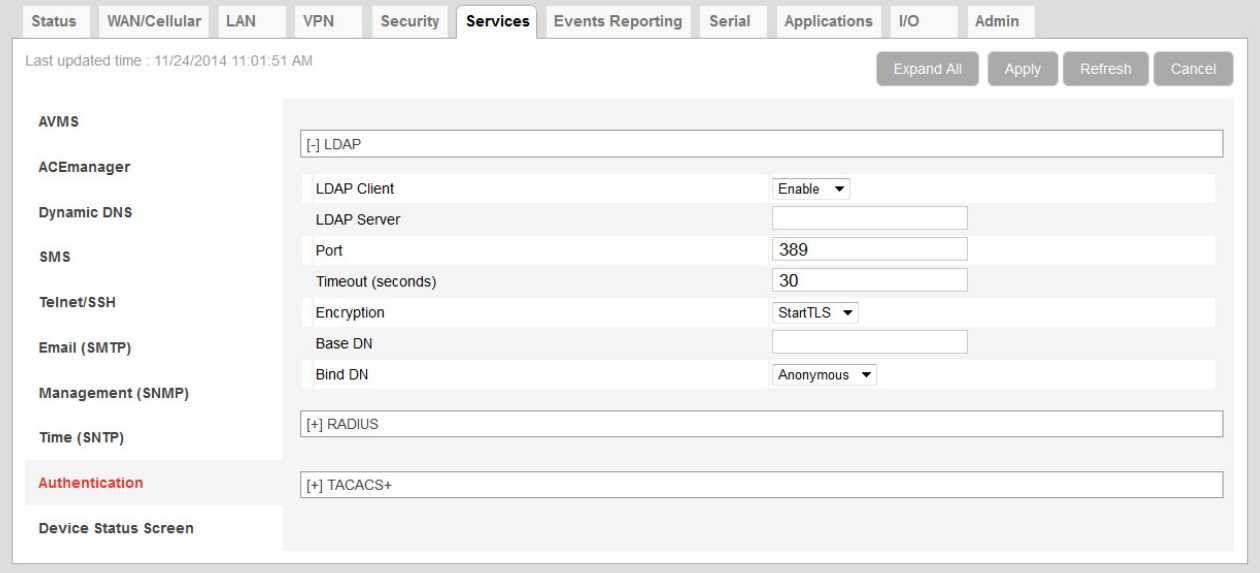


Figure 8-19: ACEmanager: Services > Authentication > LDAP

5. Configure the other fields as described in the following table.

Field	Description
Timeout (seconds)	The time limit for the server to respond • 1–60 seconds Default is 30 seconds. *Note: If the server does not respond during the timeout (no route to host, server down, network too slow etc.), the authentication fails and the next enabled authentication mechanism checks the credentials.*
Encryption	Select the encryption type Options are: • None • SSL—Secure Sockets Layer protocol —Non-standard legacy (pre-LDAPv3) encryption type • StartTLS—Secure mechanism integrated into the LDAPv3 protocol (default)
Base DN	The Base DN is the path in the LDAP tree to the list of users (example shown is dc=sierrawireless,dc=com). This is where the LDAP protocol searches for a matching user to authenticate.
Bind DN	Choose how the LDAP search is done Options are: • Anonymous—Bind anonymously (default) • Explicit—Use a specific account to bind with
Bind DN User	This field only appears if you selected Explicit in the Bind DN field The full path of the user authorized to perform requests in the LDAP database (example shown is cn=admin,dc=sierrawireless,dc=com)
Bind on Password	This field only appears if you selected Explicit in the Bind DN field User password to bind with

6. Click Apply.

RADIUS Authentication

Remote Authentication Dial In User Service (RADIUS) uses UDP and checks authentication credentials, using a shared key.

To configure RADIUS:

1. Go to Services > Authentication.
2. In the RADIUS Client field, select Enable.

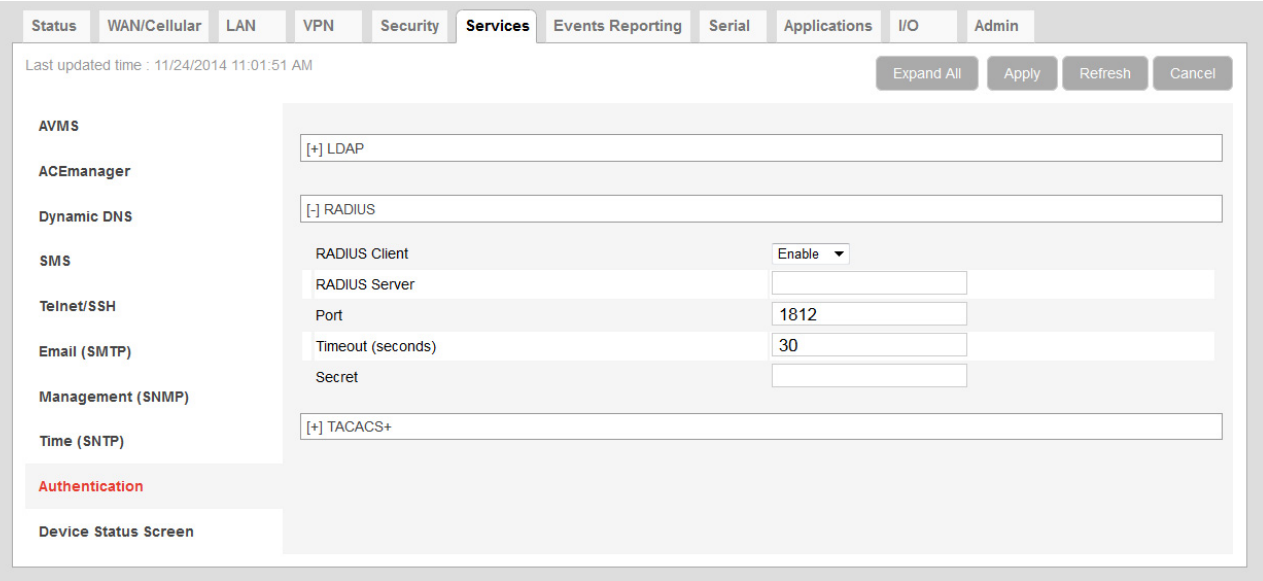


Figure 8-20: ACEmanager: Services > Authentication > RADIUS

3. Configure the other fields as described in the following table.

Field	Description
RADIUS Server	RADIUS server IP address or resolvable domain name
Port	By default, RADIUS uses UDP port 1812
Timeout (seconds)	The time limit for the server to respond • 1–60 seconds Default is 30 seconds. *Note: If the server does not respond during the timeout (no route to host, server down, network too slow etc.), the authentication fails and the next enabled authentication mechanism checks the credentials.*
Secret	Shared secret for configured server

4. Click Apply.

TACACS+ Authentication

Terminal Access Controller Access-Control System Plus (TACACS+) uses TCP protocol and encrypts the entire packet, except the header.

To configure TACACS+:

1. Go to Services > Authentication.
2. In the TACACS+ Client field, select Enable.
3. Enter:
   - The LDAP server IP address or resolvable domain name

- The Port number (default is TCP port 389)

4. Ensure that the LDAP server IP address/port is reachable not only from outside the company, but also from inside the mobile network your gateway is on.

   You can use a utility such as netcat to test this. If netcat is available try:
   nc -z <IP> <port>; echo $?

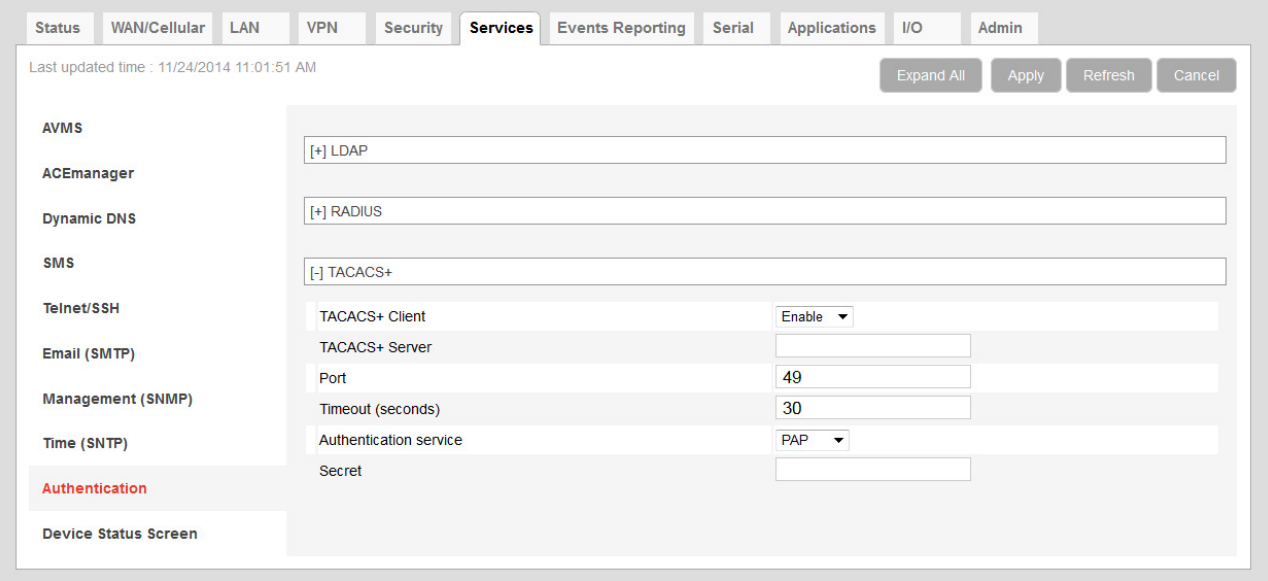


Figure 8-21: ACEmanager: Services > Authentication > TACACS+

5. Configure the other fields as described in the following table.

Field	Description
Timeout (seconds)	The time limit for the server to respond • 1–60 seconds Default is 30 seconds. *Note: If the server does not respond during the timeout (no route to host, server down, network too slow etc.), the authentication fails and the next enabled authentication mechanism checks the credentials.*
Authentication service	The type of bind used for authentication Options are: • PAP—Password Authentication Protocol (default) • CHAP— Challenge Handshake Authentication Protocol The stronger of the two protocols. Recommended, provided it is supported by all the client devices. • Login—User name and password
Secret	Shared secret for configured server

6. Click Apply.

Device Status Screen

The Device Status Screen feature, when enabled, allows you to addnetwork status parameters to the ACEmanager Login screen. Once enabled, subsequent logins to ACEmanager display whatever status parameters have been previously checked on the Device Status Screen.

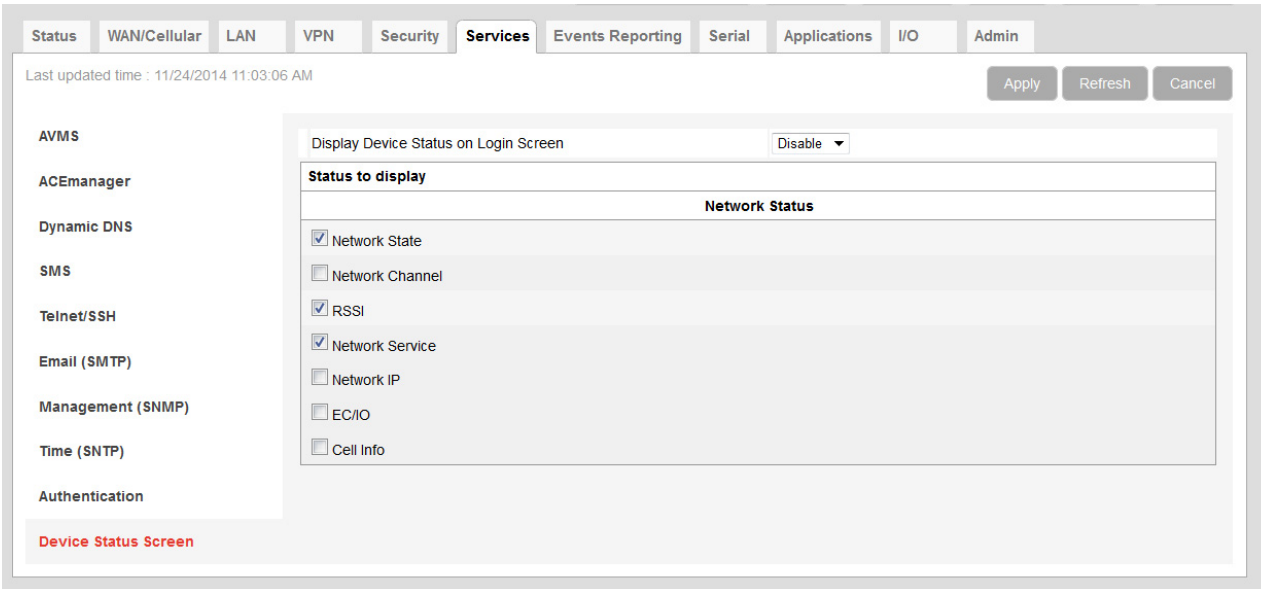


Figure 8-22: ACEmanager: Services > Device Status Screen

Field	Description
Display Device Status on Login Screen	Enables device status parameters on the login screen Options are: Disable (default) or Enable
Status to display	Allows you to display specific network status parameters on the login screen

9: Events Reporting Configuration

Introduction

You can configure the AirLink gateway to generate reports or initiate actions based on specified events. Events can either be generated internally, such as a signal quality indicator crossing a specified threshold, or by external devices attached to the analog or digital inputs.

Events that can trigger reports or actions include:

- A switch on connected equipment opens or closes (digital input)
- A pulse accumulation crosses a configured threshold
- An analog meter on connected equipment crosses a configured threshold (Analog input is reported in volts or transformed to meaningful units.)
- Changes to network status such as signal strength, network state, and network service
- The gateway's power supply (in volts) crosses a configured threshold
- The AirLink gateway board or radio temperature crosses a configured threshold
- A configured threshold for daily or monthly data usage is crossed

Depending on the type of report, reports can be sent to a local or remote report server or an email address.

Figure 9-1 summarizes how Event reporting works.

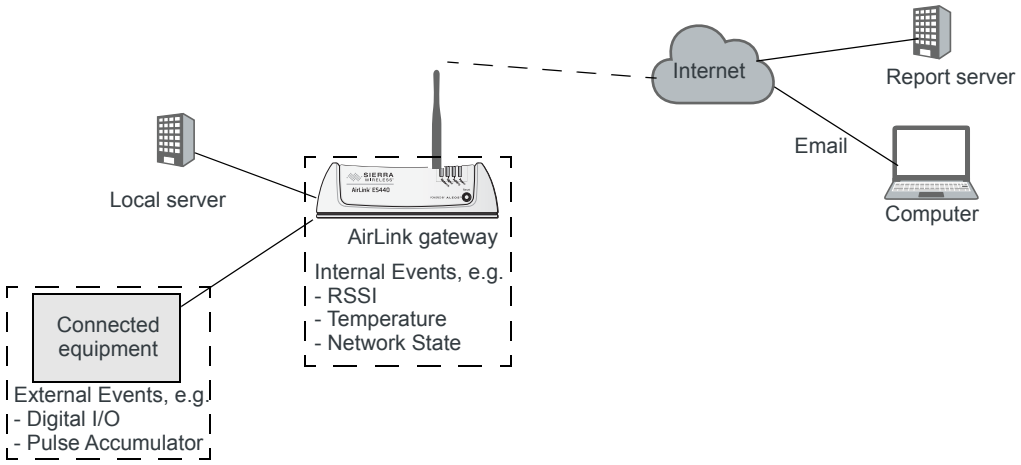


Figure 9-1: Events Reporting

Events/Actions are not one shot activities. After an Action is performed, the Event is still active and will trigger an Action the next time the state change or threshold crossing occurs.

A single Event may activate one or more Actions. For example, if RSSI is below threshold, you can send an email (Action 1) and send an SNMP TRAP (Action 2).

A single Action may be activated by one or more Events. For example, if either the network state changes to Network Ready or the RSSI crosses a configured threshold, the same Action is performed.

Configuring Events Reporting

Before you begin

If you plan to use either of the following, configure that feature in ACEmanager before configuring Events Reporting:

- Email (Email (SMTP) on page 169)
- SNMP Trap (Management (SNMP) on page 172)

Configuring Events Reporting

When configuring Events Reporting, first configure the Action (that is, how you want to be notified when the Event occurs). Then configure the Event you want reported, and finally, link the Event to the Action.

Note: All Events Reporting configuration changes take effect after a short delay (about one minute). No reboot of the AirLink gateway is necessary.

Configuring the Action

Note: You can define a maximum of 5 Actions.

Click the appropriate link for instructions on configuring the desired Action. Once the Action is configured, proceed to Event Types on page 189.

- Email
- SNMP TRAP

Email

Note: Sending an email report is limited to SMTP servers that are open and do not require a secure login.

To configure ALEOS to send an email report:

1. Ensure that email is configured on the Services > Email (SMTP) screen. (See *Email (SMTP)* on page 169.)
2. On the Events Reporting tab, select Actions from the menu on the left.
3. Enter the desired Action Name.
4. From the drop-down menu in the Action Type field, select Email.

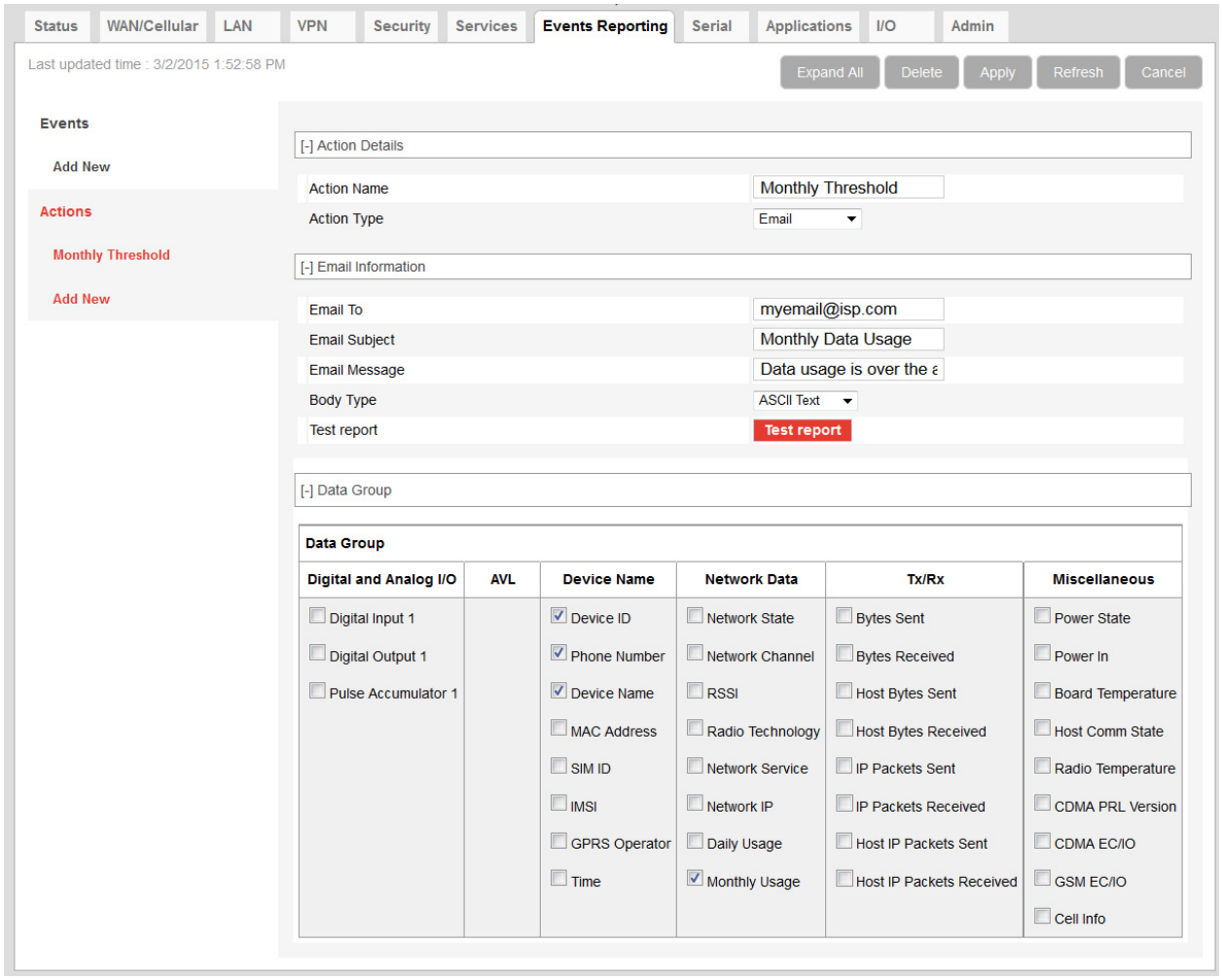


Figure 9-2: ACEmanager: Events Reporting > Action Type > Email

5. Complete the Email Information section with the recipient's email address, the subject line, and the desired message.
6. In the Body Type field, select the desired format for the Data Group information included in the report.
7. In the Data Group section, select the data to be included in the email report. For more information on the options, see Report Data Group on page 187.
8. Click Apply.

   The name you assigned to the Action appears under Actions. You can click on this anytime to modify the settings.
9. Optional—If desired, after you have updated all the fields and clicked the Apply button, wait about 1 minute, and then click the Test report button to send a test email to verify that the destination and format are correct.
10. Click Events on the menu on the left and follow the instructions on Event Types on page 189 to configure the Event you want associated with this Action and to link the Action to the Event.

SNMP TRAP

To configure ALEOS to send an SNMP TRAP notification:

1. Ensure that SNMP is configured on the Services > Management (SNMP) page. (See *Management (SNMP)* on page 172.)
2. On the Events Reporting tab, select Actions from the menu on the left.
3. Enter the desired Action Name.
4. From the drop-down menu in the Action Type field, select SNMP TRAP.

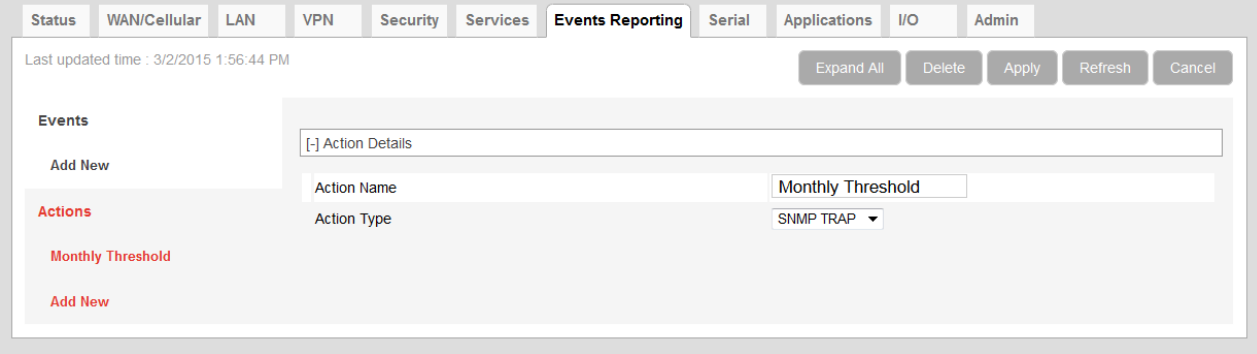


Figure 9-3: ACEmanager: Event Reporting > Action Type

5. Click Apply.

   The name you assigned to the Action appears under Actions. You can click on this anytime to modify the settings.
6. Click Events on the menu on the left and follow the instructions on Event Types on page 189 to configure the Event you want associated with this Action and to link the Action to the Event.

   If you have more than one event or action configured, the trap indicates which Event triggered which Action.

Report Data Group

For email messages, you can select the data you want to be included in the report. Check the box corresponding to the data displayed. By default, all the boxes are clear.

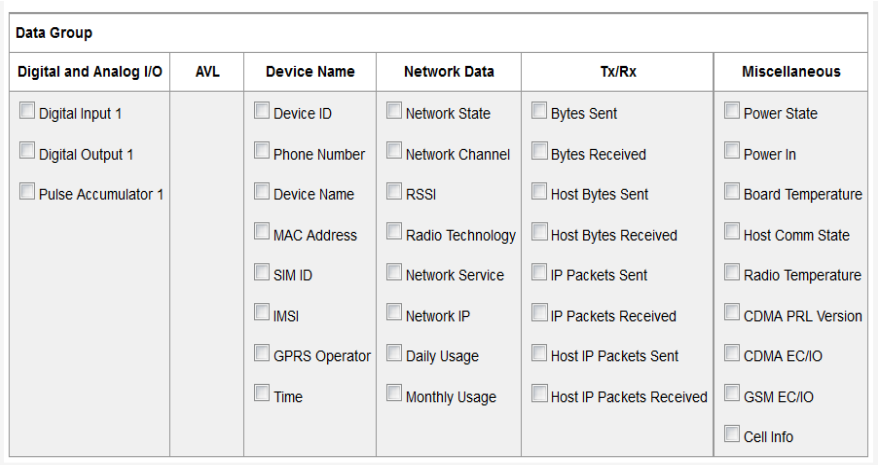


Figure 9-4: ACEmanager: Events Reporting > Action (Data Group)

The reports attributes are:

- Digital and Analog I/O
  - Include Digital Input 1—The status of the digital input
  - Include Digital Output 1—The status of the digital output
  - Include Pulse Accumulator—The pulse count for the digital input
- Device Name

  These elements in the Device Name group are general identifiers for the AirLink gateway and its cellular account.
  - Include Device ID—The device ID (serial number) for the AirLink gateway
  - Include Phone Number—The phone number of the AirLink gateway
  - Include Device Name—The name of the AirLink gateway
  - Include MAC Address—The MAC Address of the Ethernet port of the AirLink gateway
  - Include SIM ID—The SIM ID of the AirLink gateway
  - Include IMSI—The IMSI of the SIM installed in the AirLink gateway
  - Include GPRS Operator—The wireless Mobile Network Operator the SIM card is associated with
  - Include Time—The time the AirLink gateway is active
- Network Data

  The Network Data in this group relates to the mobile network and the connection state of the AirLink gateway.
  - Include Network State—The network state for the AirLink gateway
  - Include Network Channel—The network channel to which the AirLink gateway is connected
  - Include RSSI—The signal strength for the AirLink gateway
  - Radio Technology—Type of service being used by the device (e.g. EV-DO HSPA, LTE)
  - Include Network Service—The network service for the AirLink gateway
  - Include Network IP—The IP address given by the mobile network
  - Include Daily Usage —The daily usage of the AirLink gateway (Units as configured on the Applications > Data Usage screen)
  - Include Monthly Usage —The monthly usage of the AirLink gateway (Units as configured on the Applications > Data Usage screen)

- Tx/Rx

  The Network Traffic in this group relates to the mobile network and the network between the AirLink gateway and any directly connected device(s).
  - Include Bytes Sent—The number of bytes sent on the mobile network since last reset
  - Include Bytes Received—The number of bytes received from the mobile network since last reset
  - Include Host Bytes Sent—The number of bytes sent from the network between the AirLink gateway and the connected device(s) since last reset
  - Include Host Bytes Received—The number of bytes received from the network between the AirLink gateway and the connected device(s) since last reset
  - Include IP Packets Sent—The number of IP packets sent on the mobile network since last reset
  - Include IP Packets Received—The number of IP packets received from the mobile network since last reset
  - Include Host IP Packets Sent—The number of IP packets sent from the network between the AirLink gateway and the connected device(s) since last reset
  - Include Host IP Packets Received—The number of IP packets received from the network between the AirLink gateway and the connected device(s) since last reset
- Misc Data

  Miscellaneous Data includes temperature rates and other information that does not fit in the other categories
  - Power State—Current power state of the AirLink gateway (Initial, On, Low Cancellable, Low Pending 1, Low Pending 3, Low Final, Low) Refer to the Services on page 45 for details.
  - Include Power In—The voltage level of the power coming in to the AirLink gateway at the time of the report
  - Include Board Temperature—The temperature of the internal hardware of the AirLink gateway at the time of the report
  - Include Host Comm State—The signal level between the AirLink gateway and the connected device(s)
  - Radio Temperature—The temperature of the internal radio module
  - CDMA PRL Version—PRL version used by the AirLink gateway
  - CDMA EC/IO—The quality of the signal from the cellular CDMA network
  - GSM EC/IO—The quality of the signal from the cellular GSM network
  - Cell Info—The mobile network cell information for the AirLink gateway

Event Types

Note: You can define a maximum of 5 Events.

To define an Event:

1. On the Event Reporting tab, select Events > Add New from the menu on the left.

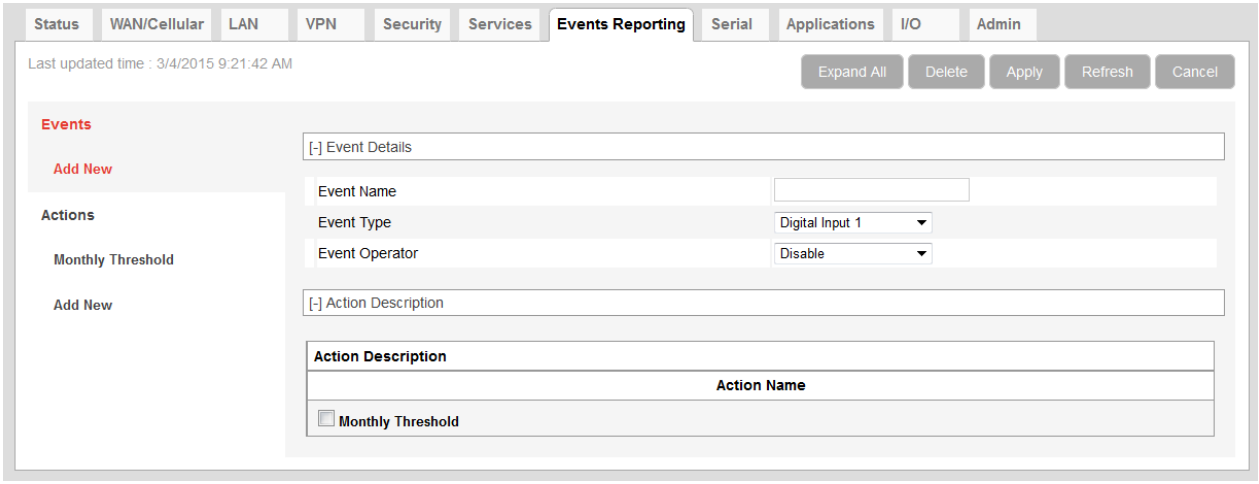


Figure 9-5: ACEmanager: Events Reporting, Events > Add New

2. Enter the desired name for the Event.
3. Select the Event type from the drop-down menu.
4. Select the Event Operator and the Value to Compare. The options available depend on the Event type you choose. See Table 9-1 on page 191 for a list of options for each Event type.
5. All the configured Actions appear at the bottom of the screen. Select the check box beside the Action you want to associate this Event with.
6. Click Apply.

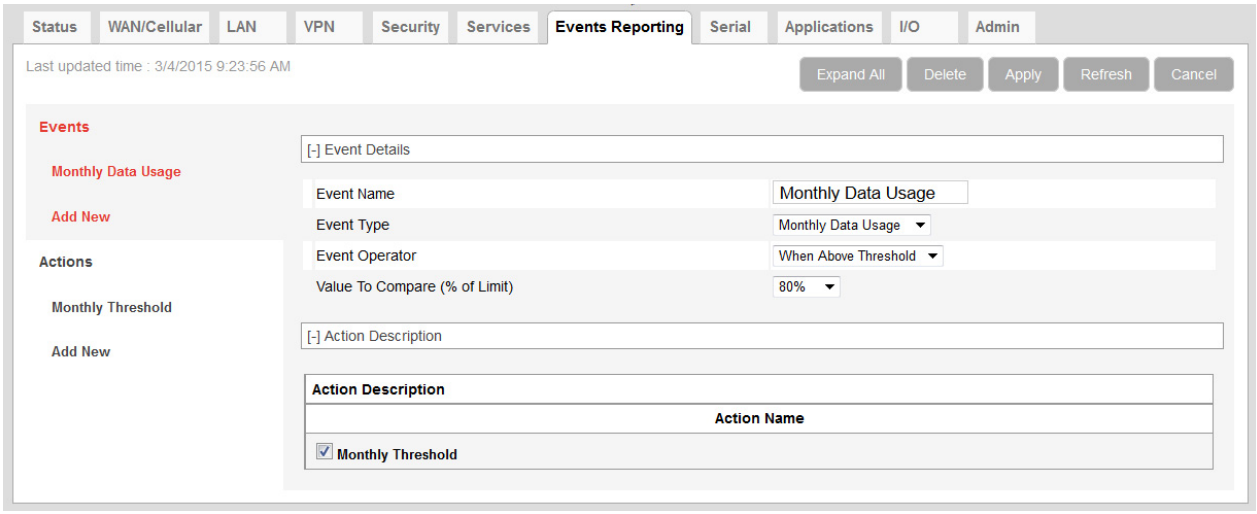


Figure 9-6: ACEmanager: Events Reporting > Events

Table 9-1: Event Types

Event Name	Event Type	Event Operator Options	Values to Compare
Digital Inputs			
Digital Input The AirLink ES Series gateway has 1 digital input.	State Change	• Disable • When Switch Closed • When Switch Opened • On any change	N/A
Pulse Accumulator The AirLink ES Series gateway has 1 pulse accumulator.	Threshold Crossing	• Disable • When Changed By	• Pulse Accumulator Delta • Starting Trigger Value
Network			
RSSI	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Signal Power (-dBm))
Network State	State Change	• Disable • When Cellular is Ready (Triggered when a cellular connection is established)	N/A
Network Service	State Change	• Disable • On Service • On No Service • On Change	Value To Compare (Network Service): • Roaming • 2G Service • Rev A or HSUPA • Any Data Service
Other Report Types			
Periodic Reports	Threshold Crossing (Time)	• Disable • Periodically	Value To Compare: Report Period (secs) *Note: The minimum interval between periodic reports is 3 seconds. Setting an interval less than 3 seconds results in only one report being sent.*
Power In	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Power In Threshold (volts))

Table 9-1: Event Types (Continued)

Board Temperature	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Temperature Threshold (°C))
CDMA HW Temperature	Threshold Crossing	• Disable • When Above Threshold • When Below Threshold • When Cross Threshold	Value To Compare (Temperature Threshold (°C))
Data Usage			
Daily Data Usage	Threshold Crossing	• Disable • When Above Threshold	Value To Compare (% of Limit)
Monthly Data Usage	Threshold Crossing	• Disable • When Above Threshold	Value To Compare (% of Limit)

Note: You can only configure one Event with either a Daily Data Usage or Monthly Data Usage trigger. If you configure more than one, for example, a trigger when the Daily Data Usage reaches a certain percentage and a trigger when the Monthly Data Usage reaches a certain percentage, only the last threshold configured is used.

ALEOS Data Usage is approximate and should not be compared with data usage recorded by the Mobile Network Operator. SIERRA WIRELESS IS NOT RESPONSIBLE FOR DATA OVERAGES.

10: Serial Configuration

Use the serial port to connect devices or computers using a DB9-RS232 connection.

Note: These commands are specific to the RS232 port and generally do not apply to USB/serial.

Port Configuration

Serial Port Configuration consists of five categories of configurable parameters:

- Port Configuration on page 193
- Advanced on page 199
- TCP on page 201
- UDP on page 203
- PPP/SLIP on page 205

Port Configuration

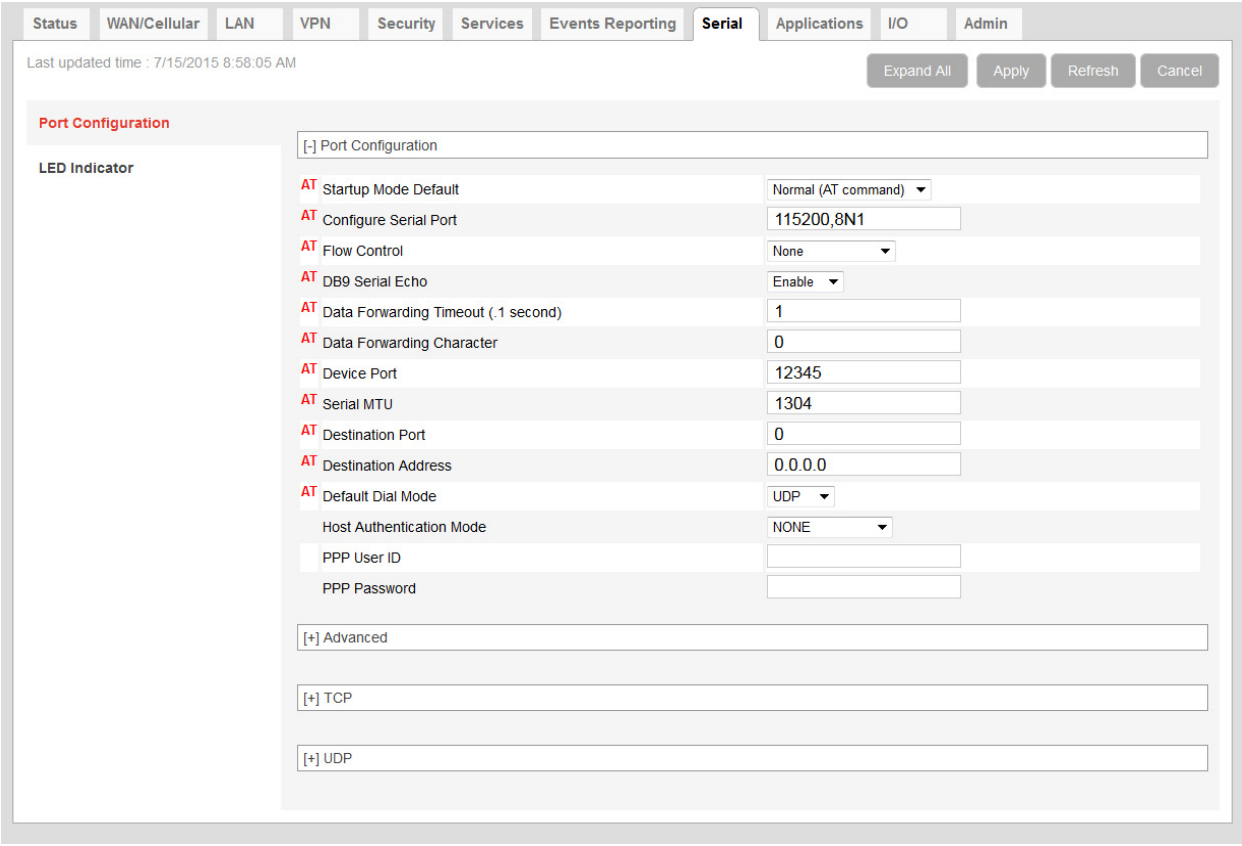


Figure 10-1: ACEmanager: Serial > Port Configuration > Port Configuration

Table 10-1: Serial Port Configuration > Port Configuration

Field	Description
Port Configuration	
Startup Mode Default	Default power-up mode for the serial port. When the AirLink gateway is power-cycled, the serial port enters the communication mode specified. *Note: It can take up to 5 minutes to establish a connection.* • Normal (AT command) (default) • SLIP • PPP • UDP • TCP • Reverse Telnet/SSH—Allows you to telnet or SSH into a router or other device connected to the AirLink gateway via a serial port. For information on configuring reverse telnet, see Reverse Telnet/SSH on page 196. UDP Multiple UnicastThis option is not supported on the ES Series gateways.You can also use an AT command to configure this field. See MD on page 315.
Autologin Reverse Telnet	This field only appears when the Startup Mode Default field is set to Reverse Telnet/SSH. Determines the log in procedure when using reverse telnet. • Enable—Do not enter a user name and password when you telnet to a a router or other device that has a serial connection to your AirLink gateway. Login is automatic. (default) • Disable—Enter a user name and password when you telnet to a a router or other device that has a serial connection to your AirLink gateway. For more information about reverse telnet, see Reverse Telnet/SSH on page 196.
Configure Serial Port	Format: [speed][data bits][parity][stop bits] Valid speeds are 300–115200, data bits: 7 or 8, parity: O,E,N,M, stop bits: 1,1.5. Default is 115200,8N1. You can also use an AT command to configure this field. See S23 on page 322.
Flow Control	Serial port flow control setting • None—No flow control is being used (default) • Hardware—RTS/CTS hardware flow control is being used • Transparent SW—Transparent software flow control. Uses escaped XON and XOFF for flow control. XON and XOFF characters in data stream are escaped with the @ character (0x40). @ in data is sent as @@. You can also use an AT command to configure this field. See \Q on page 320.
DB9 Serial Echo	AT command echo mode • Enable—Text is visible as you type (default) • Disable—Text you type is not visible You can also use an AT command to configure this field. See E on page 320.

Table 10-1: Serial Port Configuration > Port Configuration

Field	Description
Data Forwarding Timeout (.1 seconds)	The Data Forwarding Timeout feature causes ALEOS to wait until no data has been received on the serial port for the specified period of time beyond the built-in delay of 100 ms before sending a new PAD packet. Acceptable values are: 0–255. (Unit is 0.1 second; default is 1.) If the field is set to 0 or 1, the feature is disabled. ALEOS sends the new PAD packet after the built-in 100 ms delay. Data Forwarding Timeout is not applicable to AT and PPP modes.
Data Forwarding Character	PAD data forwarding character. ASCII code of character that causes data to be forwarded. Used in UDP or TCP PAD mode Default is 0 (No forwarding character). You can also use an AT command to configure this field. See S51 on page 315.
Device Port	The port on the AirLink gateway used for incoming TCP/UDP communication (Default is 12345) If either, or both, of the UDP Auto Answer or TCP Auto Answer parameters are enabled, when the AirLink gateway receives incoming TCP or UDP packets that are destined for this port, it strips off the IP header and send the packet payload out its serial port. You can also use an AT command to configure this field. See *DPORT on page 314.
Serial MTU	The serial maximum transmit unit (PAD payload) Valid range: 256–4096 bytes (Default is 1304) Recommended settings: • UDP PAD—1472 bytes • TCP PAD—1460 bytes You can also use an AT command to configure this field. See *UDPPADMTU on page 317.
Destination Port	The destination port that TCP/UDP communication is sent to You can also use an AT command to configure this field. See S53 on page 316.
Destination Address	IP address TCP/UDP communication is sent to You can also use an AT command to configure this field. See S53 on page 316.
Default Dial Mode	Protocol used to send messages Options are: • TCP • UDP (default) You can also use an AT command to configure this field. See S53 on page 316.
Host Authentication Mode	Sets the authentication method the host uses for PPP. Options are: • None (default) • CHAP—The stronger of the two protocols. Recommended, provided it is supported by all the client devices • PAP and CHAP—If CHAP is not supported by the client, the host reverts to PAP.
PPP User ID	Sets the User ID for authentication
PPP Password	Sets the User Password for authentication

Reverse Telnet/SSH

The Reverse Telnet/SSH feature allows you to connect to and configure a router or other device that has a serial connection to your AirLink gateway.

You can have only one Reverse Telnet session open at a time. If a new Reverse Telnet session is started, any existing Reverse Telnet connection will be closed.

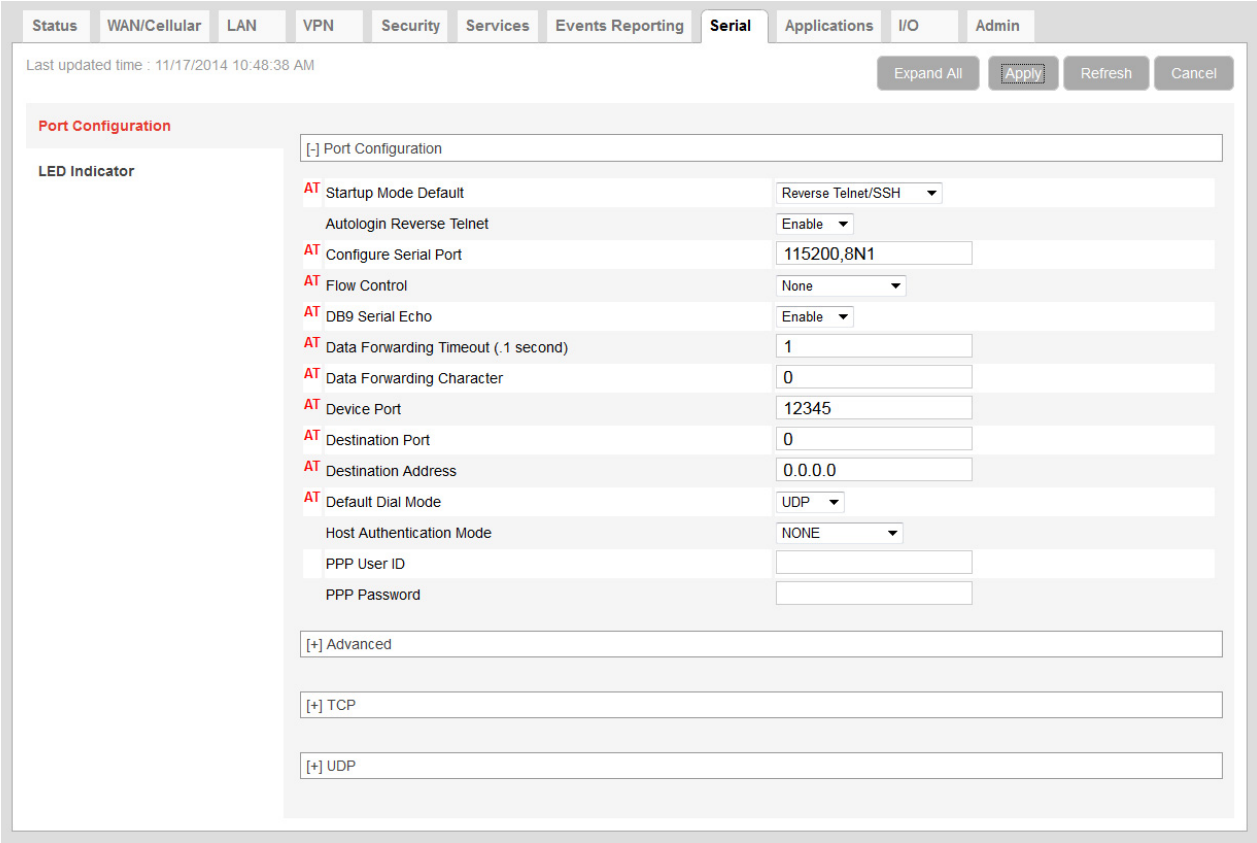
However, you can simultaneously have:

- One Telnet session for Reverse Telnet (using the port configured in the Device Port field on the Serial > Port Configuration page)
- One Telnet session for AT Commands (using the port configured in the Remote Login Server Telnet Port field on the Services > Telnet/SSH page)

Note: If you are using Reverse Telnet and you have VPNs, the more VPN tunnels in use, the greater the CPU load. This may result in lower throughput or greater delays.

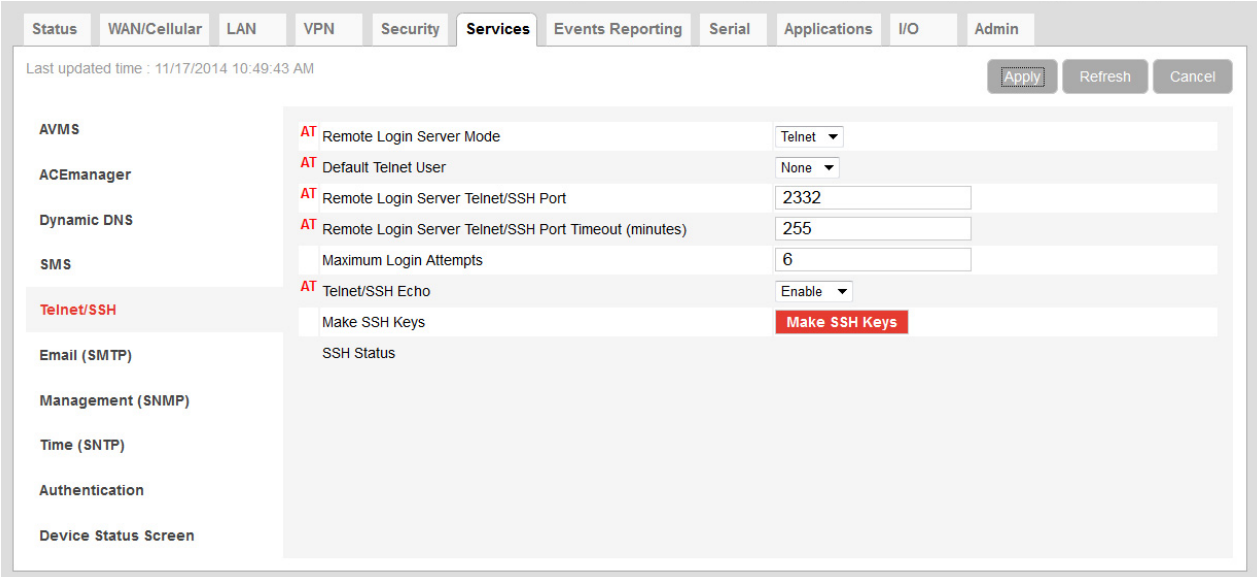
To configure Reverse Telnet/SSH:

1. Log into ACEmanager and go to Serial > Port Configuration.
2. In the Startup Mode Default field, select Reverse Telnet/SSH.
3. In the Configure Serial Port field, set the speed, data bits, parity, and stop bits. (The serial port configuration depends on the router you want to connect to. For example, to connect to a Cisco router that has a default baud rate of 9600, enter 9600,8N1 in the Configure Serial Port field.)

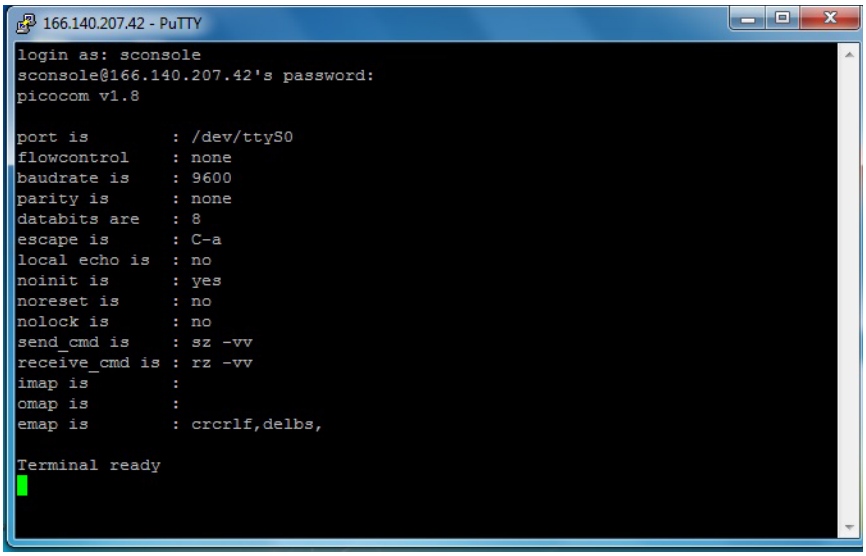


4. Optional—If you are planning to use telnet (rather than SSH), you can be automatically logged in when you telnet to the AirLink gateway without having to enter a user name and password. Autologin is not supported with SSH.
   To set up automatic login:
   a. In the Autologin Reverse Telnet field, select Enable.
   b. Click Apply.
5. Go to Services > Telnet/SSH.
6. In the Remote Login Server Mode field, select:
   - Telnet—if you want to Telnet into the connected device
   - SSH—if you want to SSH into the connected device

Note: If you enabled Autologin, select Telnet.



7. Click Apply.
8. Reboot the AirLink gateway.
9. Use a Telnet or SSH terminal client such as Putty or Teraterm to connect to the appropriate port:
   - If you are using Autologin, Telnet to the port specified in the Device Port field (default is 12345). SSH is not available with Autologin.
   - If you are not using Autologin, you can Telnet or SSH into the port specified in the Remote Login Server Telnet/SSH Port field (default is 2332).
10. If prompted, log in with the following credentials:
    - User name: sconsole
    - Password: 12345 (default)



For information on changing the default reverse telnet password, see Change Password on page 224.

ALEOS redirects you to the router or other device connected to the AirLink gateway serial port. You can use this connection to configure connected device.

Note: You may be required to enter a user name and password to access the router or other device.

Advanced

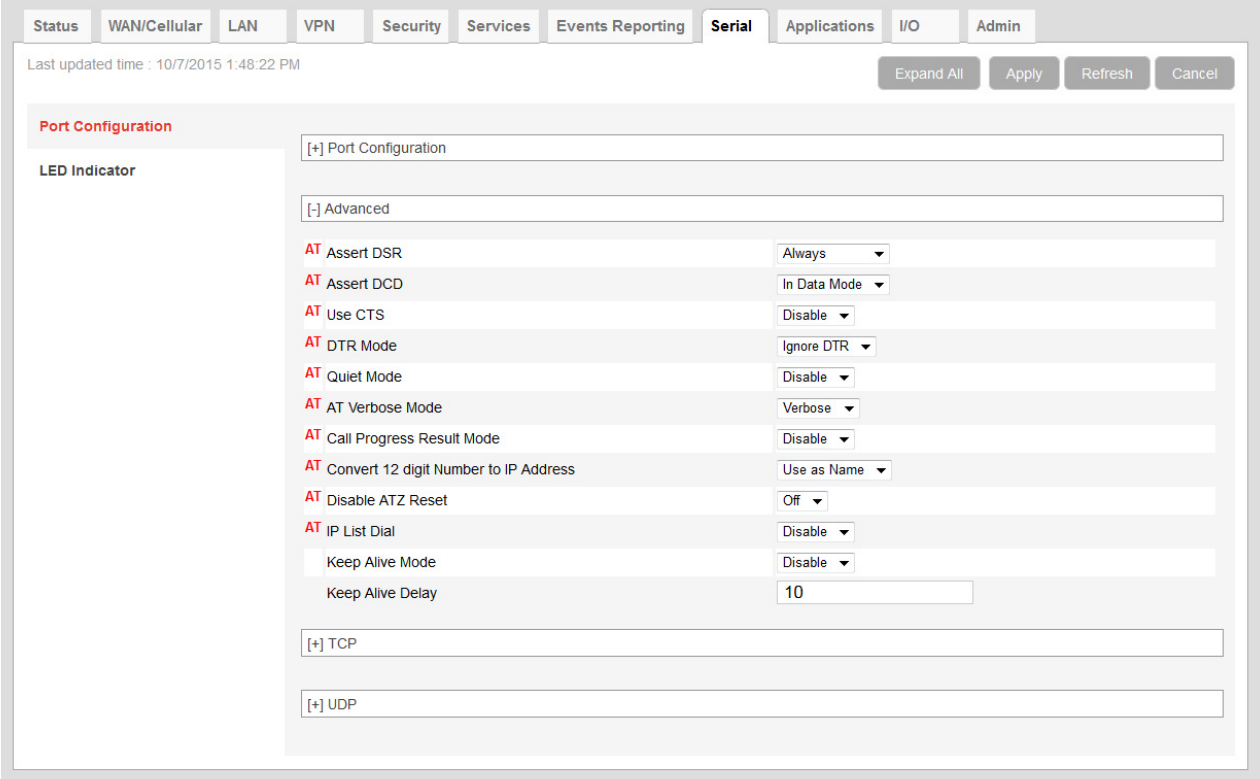


Figure 10-2: ACEmanager: Serial > Port Configuration > Advanced

Table 10-2: Serial Port Configuration > Advanced

Field	Description
Advanced	
Assert DSR	Assert DSR always when the device is in a data mode (UDP, TCP, etc.), or when the device is in network coverage. Options are: • Always (default) • In Data Mode • In Coverage You can also use an AT command to configure this field. See &S on page 320.

Table 10-2: Serial Port Configuration > Advanced

Field	Description
Assert DCD	Assert DCD always, or when the device is in a data mode (UDP, TCP, etc.) or when the device is in network coverage. Options are: • Always • In Data Mode (default) • In Coverage You can also use an AT command to configure this field. See &C on page 318.
Use CTS	Assert CTS when there is network coverage. Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See *CTSE on page 313.
DTR Mode	Use DTR from the serial device, or ignore DTR (same as S211 on page 323). Options are: • Use DTR • Ignore DTR (default)
Quiet Mode	Disable or enable display of device responses. Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See Q on page 320.
AT Verbose Mode	Sets the level of information returned for AT commands Options are: • Verbose (default) • Numeric You can also use an AT command to configure this field. See V on page 323.
Call Progress Result Mode	When enabled adds 19200 to CONNECT messages Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See X on page 323.
Convert 12 digit Number to IP Address	Choose whether a 12-digit number is converted to an IP address (eg. 111222333444 to 111.222.333.444). Options are: • Use as Name (default) • Use as IP You can also use an AT command to configure this field. See *NUMTOIP on page 315
Disable ATZ Reset	The value set in this field determines whether or not issuing an ATZ Command resets the AirLink gateway. Options are: • On — Block is enabled—ATZ does not reset the device. • Off —Block is disabled—ATZ resets the device. (default) You can also use an AT command to configure this field. See *DATZ on page 319.

Table 10-2: Serial Port Configuration > Advanced

Field	Description
IP List Dial	This allows access to the Modbus IP Address using the first two digits of the dial string. For example, ATDT1234567 would imply ID index 12 on the Modbus Address list and use the associated IP Address as the destination. Options are: • Disable (default) • Enable
Keep Alive Mode	When this feature is enabled, the AirLink gateway reboots if there is no traffic for longer than the period configured in the Keep Alive Delay field. Options are” • Disable (default) • Enable
Keep Alive Delay	When Keep Alive Mode is enabled, use this field to set the delay (in minutes) before the AirLink gateway reboots if there is no traffic on the serial port. Accepted values: • 10–65535 (Default is 10.)

TCP

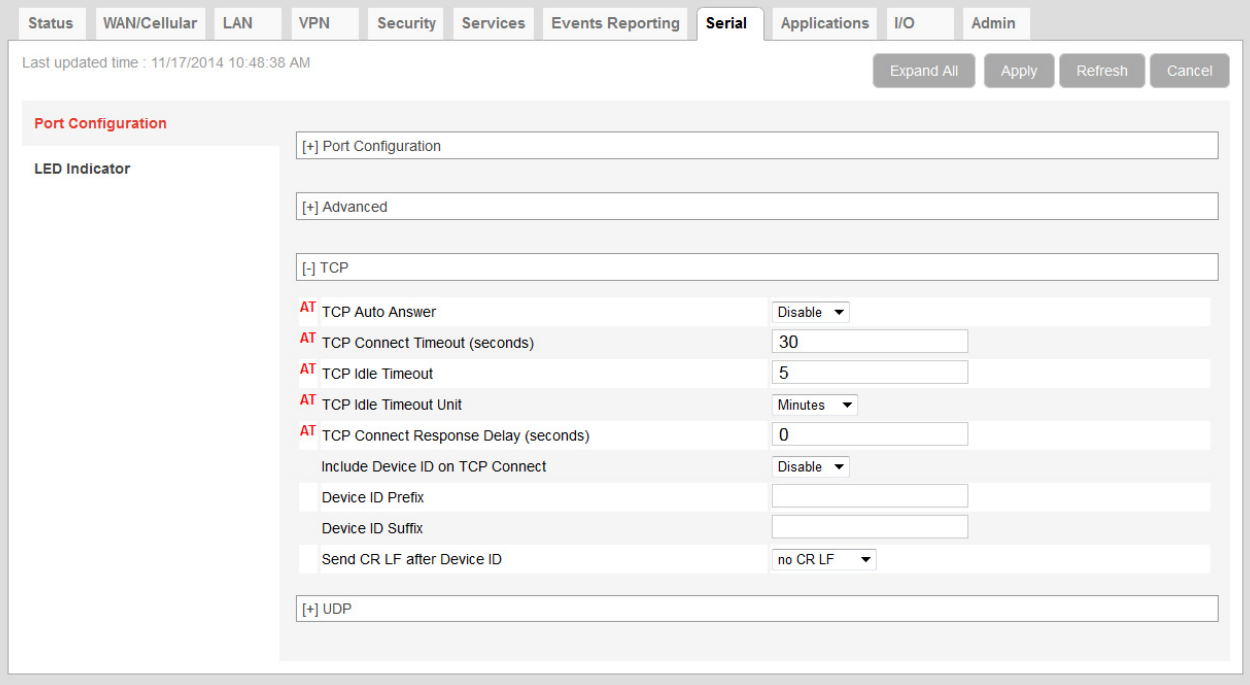


Figure 10-3: ACEmanager: Serial > Port Configuration > TCP

Table 10-3: Serial Port Configuration > TCP

Field	Description
TCP	
TCP Auto Answer	This determines how the AirLink gateway responds to an incoming TCP connection request. The AirLink gateway remains in AT Command mode until a connection request is received. The AirLink gateway sends a “RING” string to the host. A “CONNECT” sent to the host indicates acknowledgment of the connection request and the TCP session is established. • Disable (default) • Enable You can also use an AT command to configure this field. See S0 on page 321.
TCP Connect Timeout (seconds)	Specifies the number of seconds to wait for a TCP connection to be established when dialing out (Default is 30.) You can also use an AT command to configure this field.
TCP Idle Timeout	TCP idle time-out in the configured units (See TCP Idle Timeout Unit on page 202.) Specifies a time interval upon which if there is no in or outbound traffic through a TCP connection, the connection is terminated. Default is 5. You can also use an AT command to configure this field. See TCPT on page 317.
TCP Idle Timeout Unit	Units used for the TCP Idle Timeout Interval. Options are: • Minutes (default) • Seconds You can also use an AT command to configure this field. See TCPS on page 317.
TCP Connect Response Delay (seconds)	The number of seconds to delay the “CONNECT' response upon establishing a TCP connection, or the number of tenths of seconds to delay before outputting ENQ on the serial port after the CONNECT when the ENQ feature is enabled. • 0–255 (Default is 0.) You can also use an AT command to configure this field. See S221 on page 323.
Include Device ID on TCP Connect	If this option is enabled, after a TCP connection is established, ALEOS sends a packet that contains the device ID (and optionally a prefix, suffix, and CRLF). Options are: • Disable (default) • Enable
Device ID Prefix	Sets the Prefix DID in the device identification packet upon TCP connection. Maximum length of the prefix is 80 characters.
Device ID Suffix	Sets the Suffix DID in the device identification packet upon TCP connection. Maximum length of the suffix is 80 characters.
Send CR LF after Device ID	Enables a carriage return to be inserted in the device identification packet after the Suffix DID. Options are: • no CR LF • send CR • send CR LF (carriage return, line feed) Default

UDP

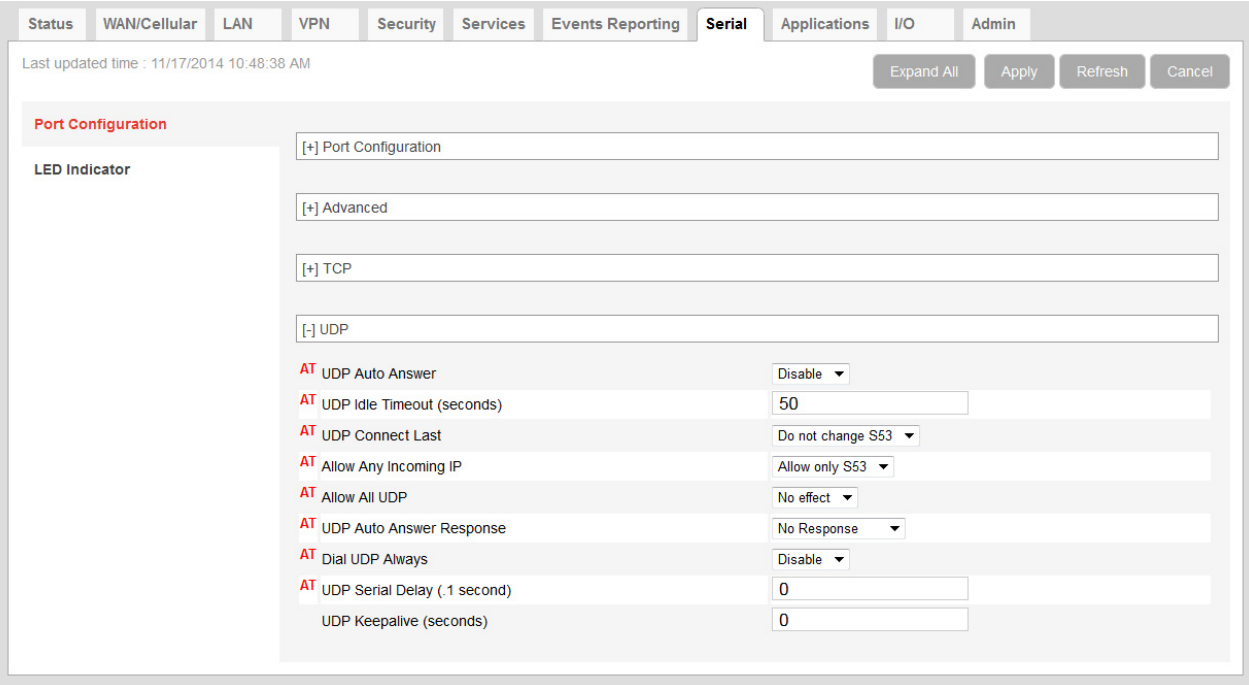


Figure 10-4: ACEmanager: Serial > Port Configuration > UDP

Table 10-4: Serial Port Configuration > UDP

Field	Description
UDP	
UDP Auto Answer	Whether the AirLink gateway auto answers and incoming UDP connection request Options are: • Disable (default) • Enable You can also use an AT command to configure this field. See S82 on page 316.
UDP Idle Timeout (seconds)	UDP Idle Time-out in seconds Specifies a time interval upon which if there is no in or outbound traffic through a UDP connection, the connection is terminated. • 0— No idle time-out • 1–255 Time-out in seconds (Default is 50.) You can also use an AT command to configure this field. See S83 on page 316.

Table 10-4: Serial Port Configuration > UDP

Field	Description
UDP Connect Last	Allows you to choose to use the last accepted IP address and port number as the default settings, instead of using S53 (destination address) Options are: • Do not change S53 (default) • Set S53 last IP *Note: Resetting the device restores the configured S53 (destination address).* You can also use an AT command to configure this field. See *UDPLAST on page 317.
Allow Any Incoming IP	When UDP auto answer is enabled, use this field to select whether to allow any incoming IP address to connect or to only allow the configured destination IP address to connect. Options are: • Allow only S53 (default) • Allow any IP address If you select Allow only S53, the Destination Port and Destination Address fields under Serial > Port Configuration must be configured. (See Table 10-1 on page 194.) You can also use an AT command to configure this field. See AIP on page 313.
Allow All UDP	Accepts UDP packets from all IP addresses when a UDP session is active. If there is no UDP session active, an incoming UDP packet is treated according to the UDP auto answer and AIP settings. Options are: • No effect (default) • Allow all—The AirLink gateway accepts all UDP traffic from any IP address during a UDP session. You can also use an AT command to configure this field. See *UALL on page 317.
UDP Auto Answer Response	Half-Open Response—In UDP auto answer (half-open) mode. Options are: • No Response—No Response codes when UDP session is initiated (default) • RING CONNECT—RING CONNECT response codes sent out serial link before the data from the first UDP packet *Note: Quiet Mode must be Off.* You can also use an AT command to configure this field. See HOR on page 320.
Dial UDP Always	The dial command always uses UDP, even when using ATDT. Options are: • Disable—Dial using the means specified (default) • Enable—Dial UDP always, even when using ATDT *Note: When this parameter is set you cannot establish a TCP PAD connection.* You can also use an AT command to configure this field. See *DU on page 314.
UDP Serial Delay (.1 second)	Waits the specified delay before sending the first received UDP packet and the subsequent UDP packets out to the serial port (in 100 ms units). • No UDP packet delay (default) • 1–255— Delay in 100ms units, from 100 ms to 25.5 sec. You can also use an AT command to configure this field. See *USD on page 317.

Table 10-4: Serial Port Configuration > UDP

Field	Description
UDP Keepalive (seconds)	Use this field to configure the time interval (in seconds) for sending UDP keepalive packets. Options are: • 1–65535—ALEOS sends a UDP packet, containing the AirLink gateway's IMEI (in little endian) to the configured Destination IP Address:Destination Port when the UDP connection is first established and then at the configured interval. If the AirLink gateways WAN IP address changes, a UDP packet is sent and the timer is reset. • 0—UDP Keepalive is disabled. (default)
UDP Recovery Ping	If an IP is provided in this field and no UDP packets are received from the server for the UDP Idle Timeout period, the gateway sends a single ping to this IP. This functionality is designed to resolve a known issue where a Verizon Wireless GX440 becomes temporarily unreachable from the mobile network after a period of time in which no data is sent or received.

PPP/SLIP

Use Point-to-Point Protocol (PPP) or Serial Line Internet Protocol (SLIP) to establish a connection between a host PC serial port and the AirLink gateway, as shown in Figure 10-5.

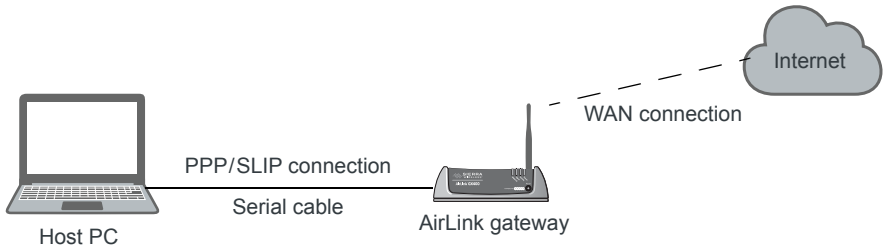


Figure 10-5: PPP/SLIP connection

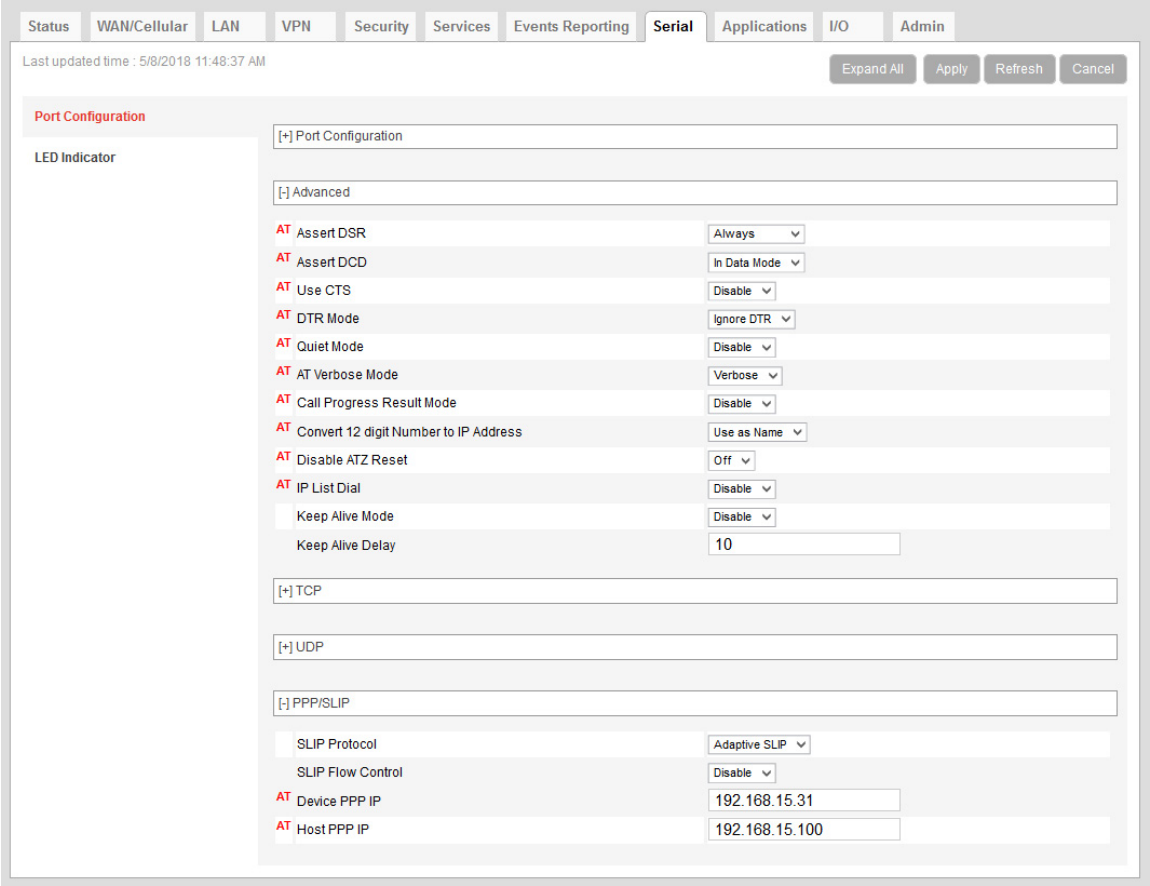


Figure 10-6: ACEmanager: Serial > Port Configuration > PPP/SLIP

Table 10-5: Serial Port Configuration > PPP/SLIP

Field	Description
PPP/SLIP This section is only visible when PPP or SLIP is selected in the Startup Mode Default field.	
SLIP Protocol	This field only appears when SLIP is selected in the Startup Mode Default field. Select the type of Serial Line Internet Protocol (SLIP) to use Options are: • Adaptive SLIP—Allow the kernel to determine the SLIP protocol (default) • SLIP—Traditional SLIP encapsulation • CSLIP—SLIP encapsulation with Van Jacobsen header compression • SLIP6—SLIP encapsulation with six-bit encoding • CSLIP6—SLIP encapsulation with Van Jacobsen header compression and 6-bit encoding

Table 10-5: Serial Port Configuration > PPP/SLIP

Field	Description
SLIP Flow Control	This field only appears when SLIP is selected in the Startup Mode Default field. Choose the SLIP data flow control setting. Options are: • Disable (default) • Enable Flow control enables the receiving device to control the data flow. This is useful if the receiving device has a heavier traffic load or less processing power than the sending computer.
Device PPP IP	Sets the device IP address (in private mode) Default is 192.168.15.31 You can also use an AT command to configure this field. See *DEVPPP on page 314.
Host PPP IP	Sets the host IP address (in private mode) Default is 192.168.15.100 You can also use an AT command to configure this field. See *HOSTPPP on page 314.

Configuring IP to Serial with Auto Answer and Serial to IP

You can configure the AirLink gateway to:

- Auto Answer incoming TCP/IP or UDP/IP connections and send the packet payload out the AirLink gateway's serial port to a connected device
- Create and send TCP/IP or UDP/IP packets containing payload data that the AirLink gateway receives over its serial port from a connected device
- Both receive and send TCP/IP or UDP/IP packets (that is, both of the above functionalities)

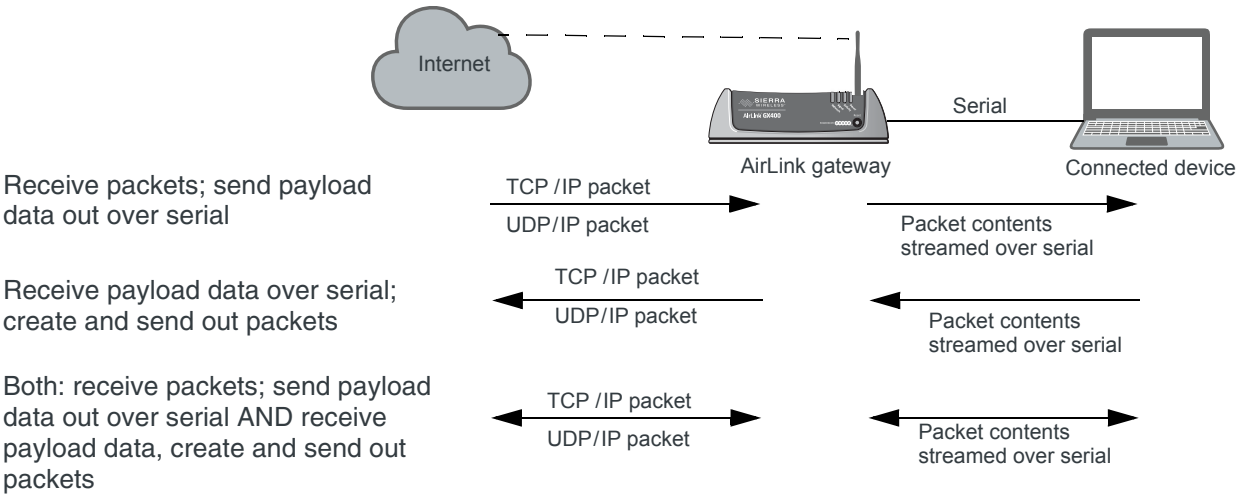
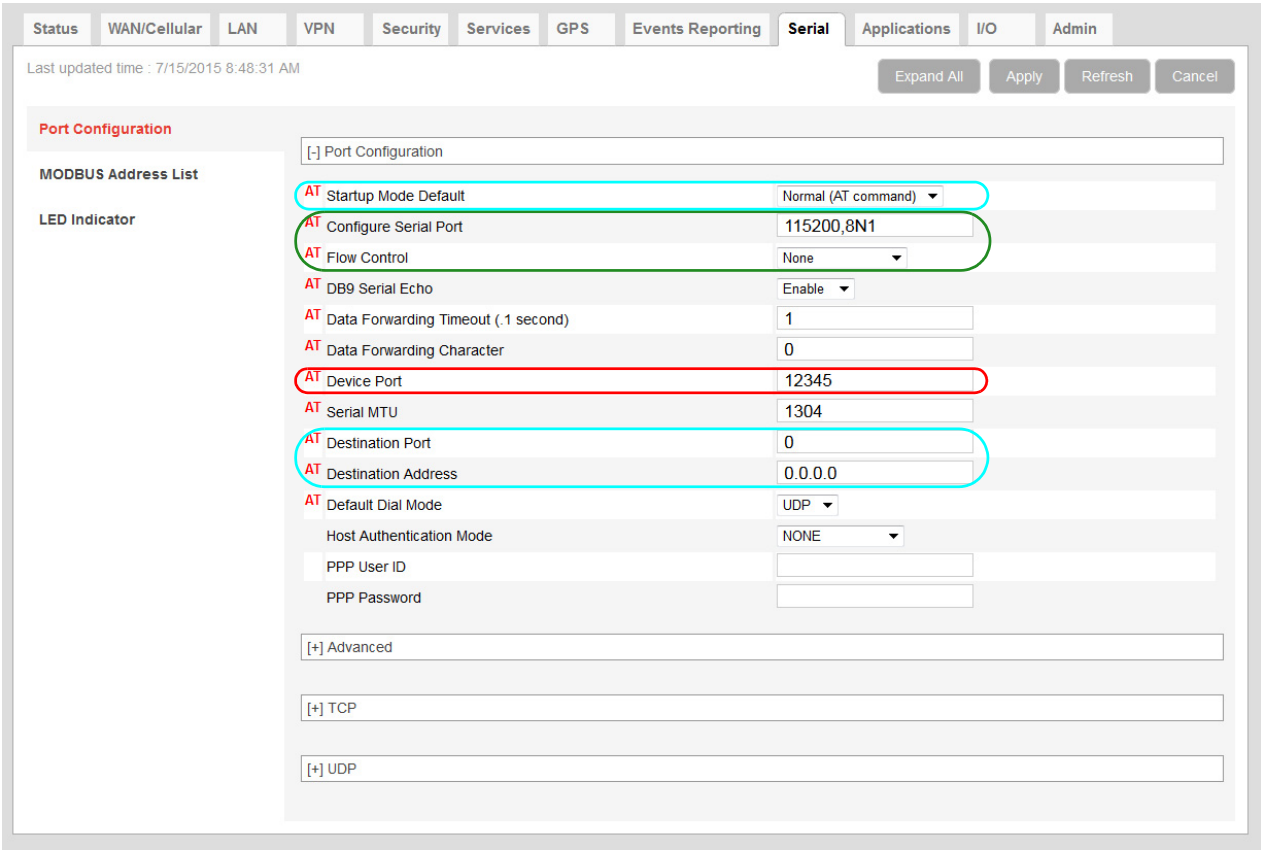


Figure 10-7: TCP and UDP Auto Answer

To configure the AirLink gateway for TCP/UDP auto answer, sending IP packets or both:

1. In ACEmanager, go to Serial > Port Configuration.



Required fields for receiving data payloads over serial, creating IP packets to send

Required fields for receiving IP packets and sending out data payloads over serial

Required fields both receiving data payloads over serial, creating IP packets to send and receiving data payloads over serial, creating IP packets to send

Figure 10-8: ACEmanager: Serial > Port Configuration

2. Use Table 10-6 and the instructions following the table to configure the desired options for this feature.

Table 10-6: Quick Guide to Configuring IP to Serial with Auto Answer and Serial to IP

Field	To receive packets and send data payload out over serial	To receive data payloads over serial and send out packets	Both (to receive packets - send out data payload AND receive data payload and send out packets)
Startup Mode Default See step Step 3.	N/A	UDP or TCP	UDP or TCP
Configure Serial Port See Step 4.	115200,8N1	115200,8N1	115200,8N1
Flow Control See Step 5.	None	None	None
Device Port See Step 6.	12345	N/A	12345

Table 10-6: Quick Guide to Configuring IP to Serial with Auto Answer and Serial to IP

Field	To receive packets and send data payload out over serial	To receive data payloads over serial and send out packets	Both (to receive packets - send out data payload AND receive data payload and send out packets)
Destination Port See Step 7.	N/A	Required	Required
Destination Address See Step 8.	N/A	Required	Required

3. Startup Default Mode—When the Startup Mode is set to UDP or TCP, the AirLink gateway takes any data sent to its serial port by a connected device and encapsulates it into a TCP/IP or UDP/IP packet.
4. Configure Serial Port—Set the baud rate of the serial port on the AirLink gateway so that it matches the baud rate of the serial port on the connected device. (The default baud rate is 115200 bps.) You can also use this field to set the framing characteristics for the serial port communication on those rare occasions when the default value of 8N1 does not apply.
5. Flow Control—This field can usually be left at the default value (None) as most serial devices use only a 3-wire connection (Tx, RX, and Gnd). However, if the serial device uses the RTS and CTS pins on the serial connection to control data flow between the two devices, set this field to Hardware.
6. Device Port—Data received on a TCP/IP or UDP/IP connection to the configured Device Port is sent out the serial port. The default value for the port:
   - On the AirLink gateway is 12345
7. Destination Port—The AirLink gateway uses the port value specified in this field to determine which port it sends the IP packet containing the data payload to. The AirLink gateway enters the value in the Destination Port field in the header of the IP packet it creates.
8. Destination Address—The AirLink gateway uses the IP address specified in this field to determine the IP address to send the packet it creates to. The AirLink gateway enters this IP address in the header of the IP packet it creates.
9. If you are configuring the AirLink gateway to:
   - Create and send packets only, go to step Step 10.
   - Receive TCP/UDP packets, complete the following instructions.

For Receiving TCP/IP Packets:

a. Expand the +TCP section of the screen.

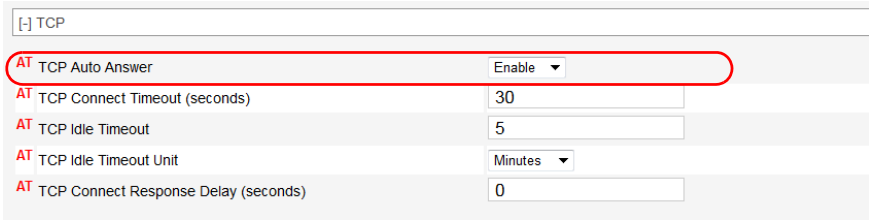


Figure 10-9: ACEmanager: Serial > Port Configuration > TCP

b. Set the TCP Auto Answer field to Enable.

For Receiving UDP/IP Packets:

a. Expand the +UDP section of the screen.

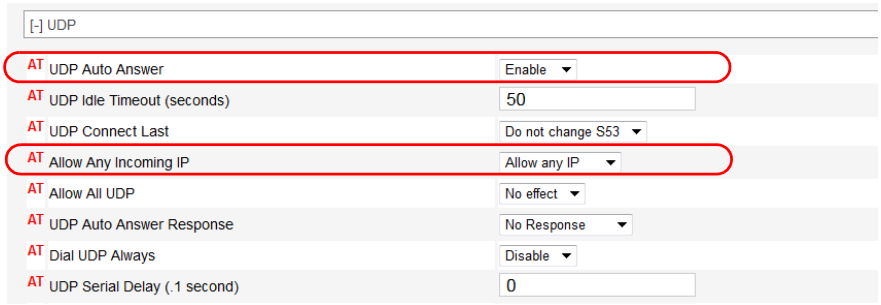


Figure 10-10: ACEmanager: Serial > Port Configuration > UDP

b. Set the UDP Auto Answer field to Enable.

c. Set the Allow Any Incoming IP field to Allow Any IP. (If this field is left at the default value, the AirLink gateway only accepts incoming UDP/IP packets from the IP address specified in the Destination Address field in the Port Configuration section of the screen.

10. For information on the other parameters, see Port Configuration on page 193.

11. Click Apply.

12. Click Reboot (in the upper right of the screen).

13. Once the reboot is complete, this feature is enabled.

If the packet contents are not being sent to the connected device, see the troubleshooting information in TCP/IP and UDP/IP Auto Answer on page 343.

LED Indicator

You can configure the Activity LED on the AirLink gateway to flash red when traffic is being transmitter or received over the serial port.

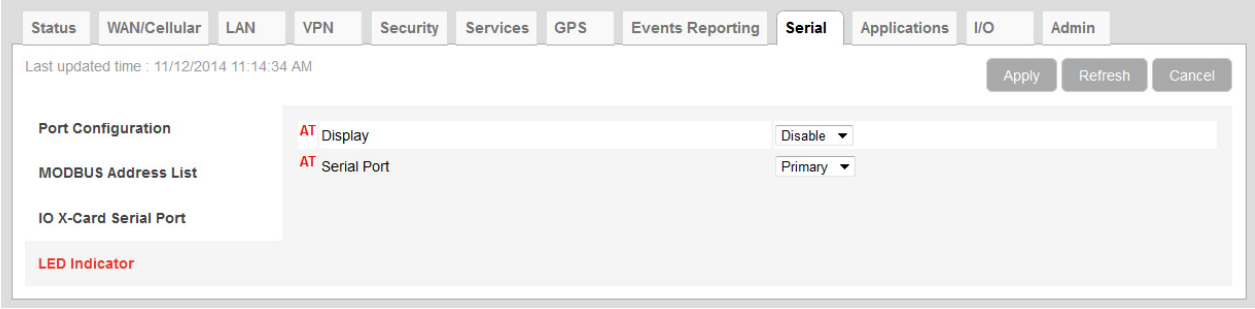


Figure 10-11: ACEmanager: Serial > LED Indicator

Table 10-7: Serial > LED Indicator

Field	Description
Display	Options are: • Disable (default) • Enable If this field is set to Enable, the Activity LED on the AirLink gateway flashes red when traffic is being transmitted/received on the serial port selected in the Serial Port field. **Activity LED** / **Traffic** Off / No traffic Flashing Green / Traffic on WAN interface Flashing Red / Traffic on selected serial port Flashing Yellow / Traffic on both the WAN interface and selected serial port You can also use an AT command to configure this field. See *SERIALLEDDISPLAY on page 316. For a complete list of LED behavior, refer to the AirLink gateway Hardware User Guide.
Serial Port	If you have an AirLink GX device with an I/O X-Card installed, use this field to select the serial port you want the LED to indicate traffic on. • Primary—Serial port on the AirLink gateway itself (default) • X-Card—Serial port on the I/O X-Card installed on the AirLink GX Series gateway For all other AirLink gateways, leave this field set to the default value.

11: Applications Configuration

The Applications tab consists of a Data Usage section and an ALEOS Application Framework section.

Data Usage

Note: Before configuring Data Usage, ensure that the AirLink gateway receives date and time information from the mobile network. You can also use the ACEmanager SNTP client to receive time from an SNTP server. (See Time (SNTP) on page 177.) If necessary, contact your Mobile Network Operator to confirm that the mobile network provides date and time information to connected devices.

The Data Usage feature on the Applications tab in conjunction with Events Reporting provides you with a way to actively monitor cellular data usage.

Once data usage is configured, you can use event reporting to:

- Actively monitor the cellular data usage by configuring monthly and/or daily usage level thresholds that result in notifications being sent to you (e.g. email or SNMP Trap) when the threshold is reached.

Note: You can configure Events Reporting to notify you when the threshold set in Data Usage is reached, but ALEOS does not block further access to the mobile network.

Note: ALEOS Data Usage is approximate and should not be compared with data usage recorded by the Mobile Network Operator.
Sierra Wireless is NOT responsible for data overages.

Step 1—Configure Data Usage

1. In ACEmanager, go to Applications > Data Usage.
2. In the Usage Monitoring field, select Enable.
3. Enter the desired values in the Daily or Monthly Limit fields (in GB or MB), and the day of the month that the billing cycle starts. For more details, see the table starting on page 213.
4. Click Apply.

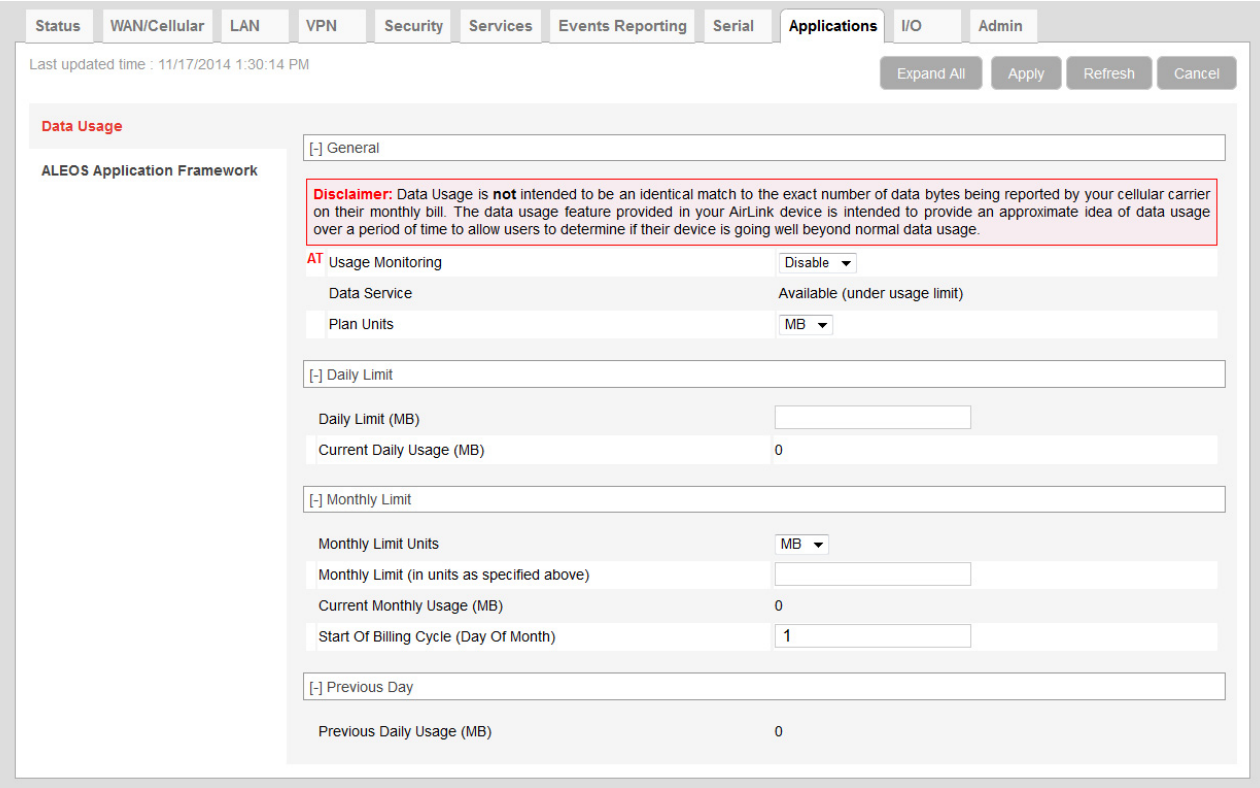


Figure 11-1: ACEmanager: Applications > Data Usage

Field	Description
General	
Usage Monitoring	Use this field to enable or disable data usage monitoring. Options are: • Disable (default) • Enable
Data Service	Available (under usage limit)—Always appears "Available (under usage limit)" in this field does not indicate that the Daily Limit and Monthly Limit Limits have not been exceeded.
Plan Units	Select the units used for your data plan. The options are: • MB—Megabytes (default) • KB—Kilobytes *Note: When you change the units in this field, the units for values in the Daily Limit and Monthly Limit fields are not converted and must be updated manually.*

Field	Description
Daily Limit	
Daily Limit (MB) **Daily Limit (KB)**	This is the user-specified daily (24 hour) data usage limit (in MB or KB, depending on the value in the Plan Units field). You can specify data usage limits on a daily basis. A limit is essentially a threshold that can trigger the software to take a user-specified action if the usage goes above the threshold. See Events Reporting Configuration on page 184. *Note: The Daily Limit value MUST be expressed as an integer (i.e., a whole number) and NOT as a fraction (e.g., "3.5").* *Note: Daily usage is cleared at midnight, UTC.* **Caution:** *Data usage limits are approximate and based on reporting conditions in ALEOS. Data usage may run over the amount set in this field before the action specified for the threshold trigger takes effect.* **Tip:** *ALEOS reads the data usage every 3 to 5 minutes. If you are using an application that requires high data usage, you can set an alert to warn you when data usage reaches a safe limit that takes into account the amount of data expected over the 3 to 5 minutes between data usage readings. For information on how to set an alert or other action, see Events Reporting Configuration on page 184.*
Current Daily Usage (MB) **Current Daily Usage (KB)**	Displays the current daily data usage (in MB or KB, depending on the option selected in the Plan Units field) *Note: Data usage includes data sent and data received.*

Field	Description
Monthly Limit	
Monthly Limit Units	Select the units for monthly data usage—MB (default) or GB. This field only appears when Plan Units on page 213 is set to MB.
Monthly Limit (in units as specified above)	This is the user-specified monthly data usage limit (in MB or GB, depending on the option selected in Monthly Limit Units). Data usage accumulates on a monthly basis and on the date you specified (the "rolling month"). Data usage accumulates during the month until the end of the next billing period, at which point the data usage totals are reset. *Note: The Monthly Limit value MUST be expressed as an integer (i.e., a whole number) and NOT as a fraction (e.g., "3.5")* *Note: Monthly usage is cleared at midnight, UTC on the last day of the billing cycle.* **Caution:** *Data usage limits are approximate and based on reporting conditions in ALEOS. Data usage may run over the amount set in this field before the action specified for the threshold trigger takes effect.*
Current Monthly Usage (MB) **Current Monthly Usage (KB)**	Displays the current monthly data usage (in MB or KB, depending on the value configured in Plan Units on page 213.) *Note: Data usage includes data sent and data received.*
Start of Billing Cycle (Day of Month)	Enter the desired start of the billing cycle. For example, 3 (Day 3 of every month) Changing the value in this field resets the Current Monthly Usage (MB) field to zero.
Previous Day	
Previous Daily Usage (MB) **Previous Daily Usage (KB)**	Shows the data usage for the previous day (in MB or KB, depending on the value configured in Plan Units on page 213.) *Note: Data usage includes data sent and data received.*

Step 2—Configure Event Reporting

1. In ACEmanager, go to Events Reporting > Actions.

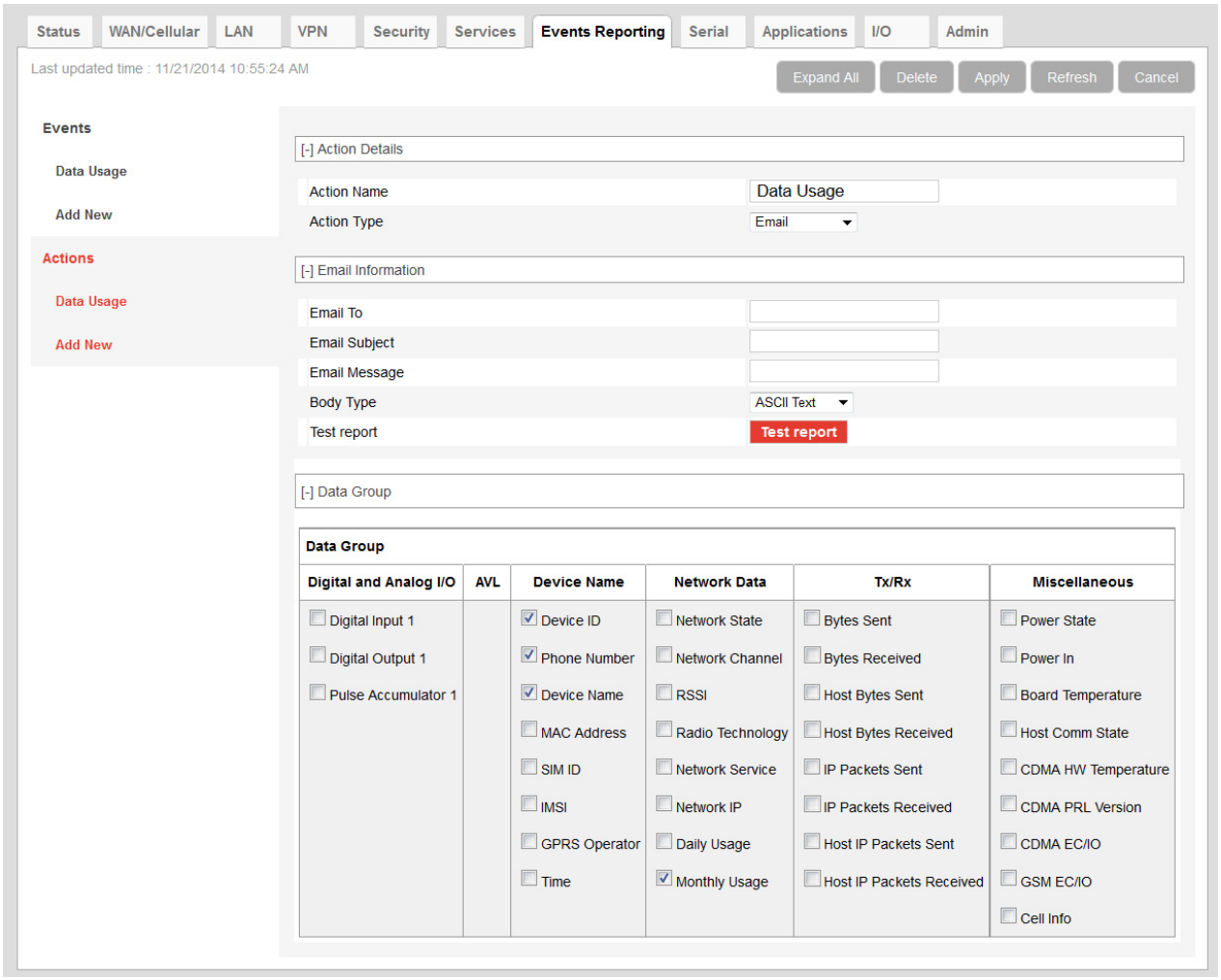


Figure 11-2: ACEmanager: Events Reporting > Events

2. Select the desired Action to be performed when the Event is triggered, such as SNMP Trap or Email, and enter the appropriate information in the related fields. For detailed instructions, see Configuring Events Reporting on page 185.
3. If you selected Email, select the check box(es) in the Data Group section of the screen to indicate the information to be included in the email.

Note: You can have more than one Action for a single Event, but you can only have one Daily Usage and one Monthly Usage Event.

4. Click Apply.
5. Go to Events Reporting > Events and configure a data usage threshold.

   The threshold is specified as a percentage of the monthly or daily limit. For example, if you have a monthly limit of 5 GB, and the threshold is set at 80%, then threshold is

reached at 4 GB of data. For detailed instructions, see Configuring Events Reporting on page 185.

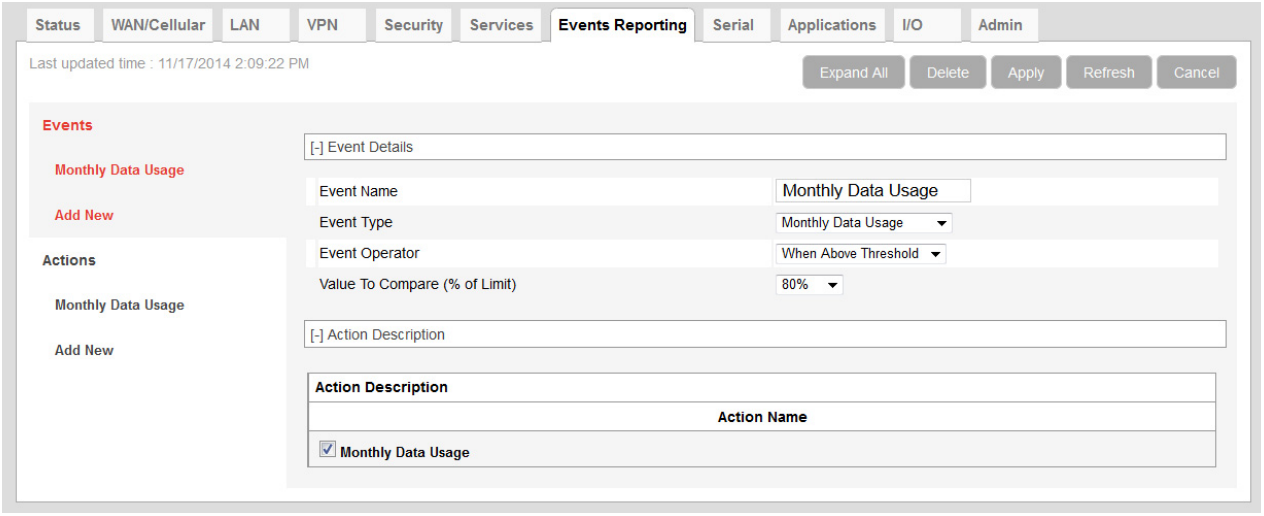


Figure 11-3: ACEmanager: Events Reporting > Events

6. At the bottom of the screen, select the check box beside the Action you want to associate the Event with.
7. Click Apply.

ALEOS Application Framework

ALEOS Application Framework (AAF) allows you to develop your own applications to run inside an AirLink gateway and leverage the ALEOS Application Platform (source.sierrawireless.com/resources/airlink/aleos_af/aleos_af_home/) or a customer-developed server platform.

Sierra Wireless gateways come without an AAF user password. Before using AAF, go to Admin > Change Password to set up an AAF user password. See AAF User Password on page 225. This password is used to install an AAF application from DevStudio onto the gateway via Secure Copy Protocol (SCP).

Once the AAF user password is set up, embedded and server application developers can start using AAF by accessing the Sierra Wireless Developer Zone (source.sierrawireless.com/resources/airlink/aleos_af/aleos_af_home/).

You may want to reserve the serial port for an AAF application. To do so, select Enable in Applications > ALEOS Application Framework > Serial Port Reserved.

It is not necessary to reserve the serial port before activating AAF.

Reserving the serial port is mandatory only if the AAF application will be using the serial port.

Note: When you reserve the serial port for AAF, it cannot be used for any other serial-related ALEOS features.

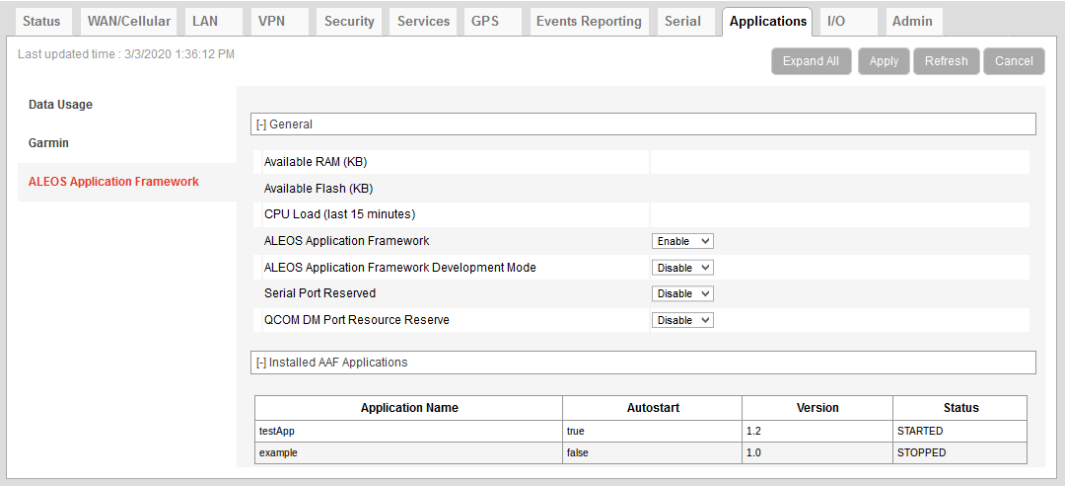


Figure 11-4: ACEmanager: Applications > ALEOS Application Framework

Field	Description
General	
Available RAM (KB)	Available RAM in kilobytes (1000 bytes), updated every 30 seconds
Available Flash (KB)	Available Flash on the user partition in kilobytes (1024 bytes), updated every 30 seconds
CPU Load (Last 15 minutes)	CPU load, averaged over the last 15 minutes and updated every 30 seconds The CPU load relates to how many applications are attempting to execute in parallel over the 15-minute period. If the load is greater than 1, some applications are waiting for CPU capacity to become available and may be delayed in launching.
ALEOS Application Framework	Enable or disable (default) the ALEOS Application Framework (AAF). If enabled, AAF starts at boot time. When the Reset to Factory default button on the Admin > Advanced page is pressed, AAF is disabled.
ALEOS Application Framework Development Mode	Appears when ALEOS Application Framework is enabled. Enable or disable (default) the AAF Development Mode. In AAF Development Mode, you can load and debug applications using AAF Developer Studio. For system security, Development Mode should be disabled in production deployments. *Note: After changing the AAF Development Mode setting to Enabled, a warning message appears at the top of the ACEmanager screen. However, please note that development mode is actually enabled after the gateway reboots.*

Field	Description
Serial Port Reserved	Select Enable to reserve the serial port for AAF. When this field is set to Enable, the serial port cannot be used for any other serial-related ALEOS features. The options are: • Disable (default) • Enable
QCOM DM Port Resource Reserve	Reserves the QCOM DM port for AAF applications. Options are: Enable (Reserve access for AAF) or Disable (Reserve access for ALEOS). Default: Disable
Installed AAF Applications	
Application Name **Autostart** **Version** **Status**	To help you manage installed applications, the table in this section shows all the installed AAF Applications and displays the: • Application name • Autostart—true or false • Version • Status—STARTED or STOPPED If no applications are installed, the table displays the message: “No application installed or AAF not started”.

12: I/O Configuration

The I/O tab in ACEmanager applies to all Sierra Wireless AirLink gateways that feature I/O ports.

You can use the input/outputs on AirLink gateways to generate reports based on a threshold being crossed, a switch being opened or closed, or the number of times a switch has changed state.

Use the Events Reporting screen to configure reports. (See Events Reporting Configuration on page 184.) Use the I/O screen to view the current state of the digital inputs, to turn the relays on and off, and to configure the units you want used in the reports based on analog inputs.

The number of digital input/outputs depends on the device.

AirLink ES Series

The AirLink ES Series:

- Has one pin (Pin 4 on the power connector) that can be configured as a digital input/output or a relay output
- Does not support analog input

More information

For more information, refer to the Hardware Configuration User Guide for your AirLink gateway.

Digital inputs

Digital inputs monitor contact closures on a switch. This allows you to monitor changes such as:

- When a door or latch is open or closed
- When a container is full or empty
- When a switch or valve is opened or closed
- The level of fuel in a vehicle (connected to an on/off sensor)
- When the trunk of a vehicle is opened or closed

You can use Events Reporting to generate reports and actions based on the digital input values.

Volts	Interpreted as
-0.5 – 1.2	Digital 0
2.2 – 30	Digital 1

For more information on setting up reports, see Events Reporting Configuration on page 184.

Relay outputs

You can use relay outputs to trigger an intermediary switch and change the state of equipment.

Current State

The Current State screen allows you to view the current values (as of the last refresh) of analog and digital inputs, pulse counts for digital inputs, and raw and transformed values for analog inputs. You can also use this screen to change the current values for Relay outputs. This change occurs immediately without a reboot.



Figure 12-1: ACEmanager: I/O > Current State

Pulse Count

Table 12-1: I/O: Current State

Command	Description
Digital Input 1 value	Displays the current value for the digital input: • 0 —Open • 1 —Closed Digital input 1 displays the value for Pin 4 on power connector. You can also use an AT command to read these values. See *DIGITALIN1? on page 324.

Table 12-1: I/O: Current State

Command	Description
Pulse Count 1	The pulse count increments when the input value changes from high to low. Pulse count 1 displays the value for Pin 4 on power connector. *Note: To reset the pulse count to zero, reset the device to the factory defaults.*
Relay Output 1	Configure Relay Output signal. Options are: • OFF (default) The circuit is open. • Drive Action Low—equivalent to ON. The circuit is closed. Relay output 1 displays the value for Pin 4 on power connector. *Note: If the same pin can be used for input or output, be aware that changing the output setting could change the input values. For pinout information for your AirLink gateway, refer to the applicable AirLink product user guide.* You can also use an AT command (see *RELAYOUT1 on page 324), an SMS command (see [prefix]relay x y on page 329), or a RAP command (refer to the Remote Application Protocol User Guide) to configure this field. *Note: Changes to the relay outputs go into effect immediately. No reboot of the AirLink gateway is necessary.*

Pulse Count details:

- Pulses are counted on falling edge (high to low).
- Repeated pulses cannot be counted when the device is powered off, or being reset. However, a single change in state while the device is powered off or being reset is counted properly.
- To reset the pulse count to zero, reset the device to the factory defaults.

Configuration

This screen allows you to configure the initial relay settings.

For more information, refer to the Hardware Configuration User Guide for your AirLink gateway.

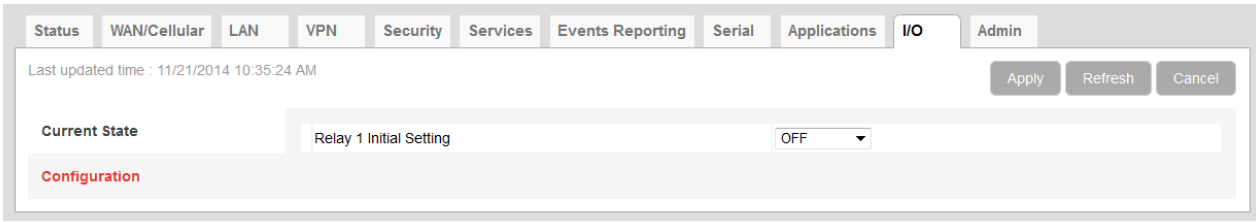


Figure 12-2: ACEmanager: I /O > Configuration

Field	Description
Relay 1 Initial Setting	The initial relay value when the AirLink gateway is powered on Options are: • ON • OFF (default) • Last Value (The value remains the same as it was before the AirLink gateway was powered down). When you change this field, the corresponding digital input value on this screen reflects the change after a screen refresh. Relay 1 Initial Setting displays the value for Pin 4 on power connector.

13: Admin

Change Password

For system security reasons, ensure that you change the default password of the AirLink gateway.

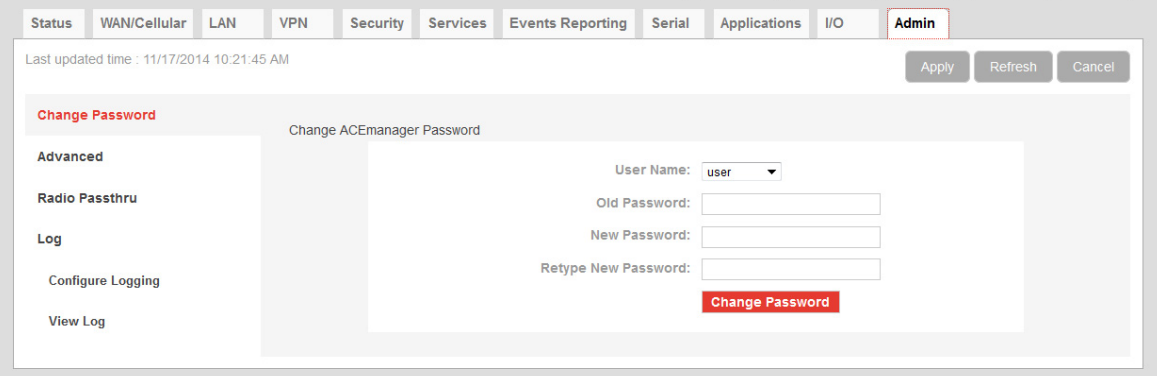


Figure 13-1: ACEmanager: Admin

To change the default password:

1. Select the User Name associated with the password you want to change: user or sconsole.

   (To create an AAF password, see AAF Password on page 332.)
2. Enter the old password.
3. Enter the new password twice.

   The password can be 4 to 32 characters long and can contain a mixture of letters, numbers, and/or special characters. The password is case sensitive.

Note: If the password is lost, the only way to recover access to the AirLink gateway is to use the hardware reset button to reset the device to the factory default settings. If the reset button has been disabled (using the Default Configuration Reset field on the Admin > Advanced screen) prior to the password being lost, the only way to recover access to the AirLink gateway is through AirVantage Management Services, for which an account is required.

4. Click Change Password.

If you want to confirm that the password has been changed, log out and then log in with the new password.

AAF User Password

An AAF user password is required if you want to use ALEOS Application Framework (AAF) to develop your own applications to run inside an AirLink gateway. This password is used when installing an AAF application from DevStudio onto the gateway.

To enter an AAF user password:

1. In ACEmanager, go to Admin > Change Password.
2. From the User Name drop-down menu, select AAF user.

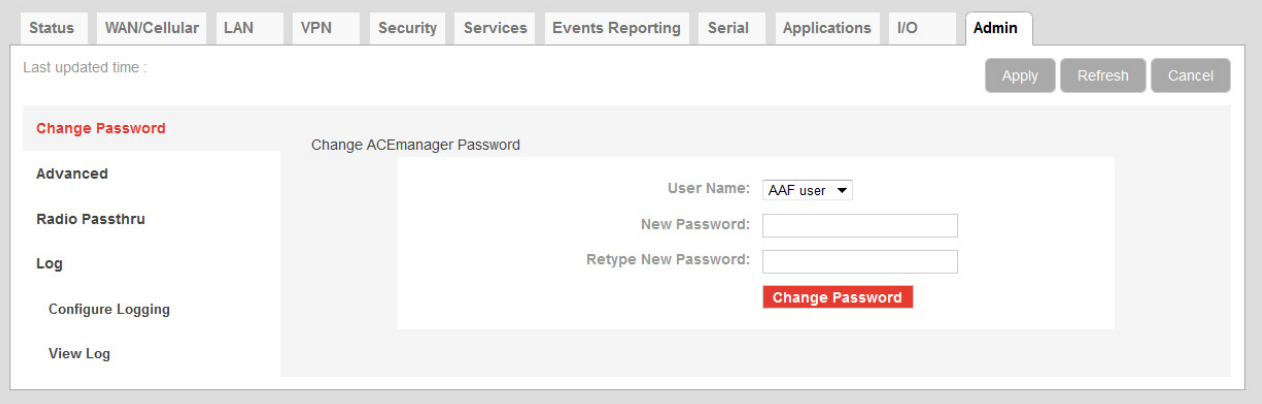


Figure 13-2: ACEmanager: Admin > Change Password > AAF user

3. Enter the new password twice and click Change Password.
4. Reboot the gateway.

For more information on using ALEOS Application Framework, see page 217.

Advanced

The Advanced screen presents features that should be rarely changed and will affect the operation of the device.

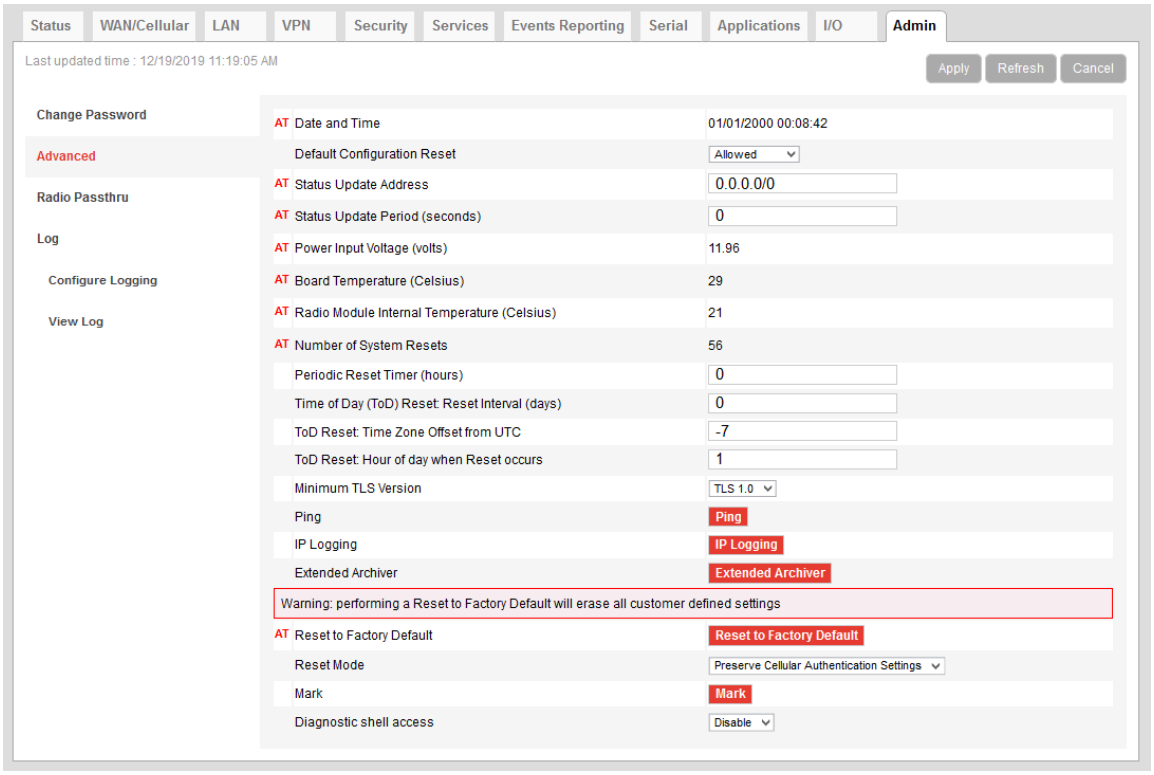
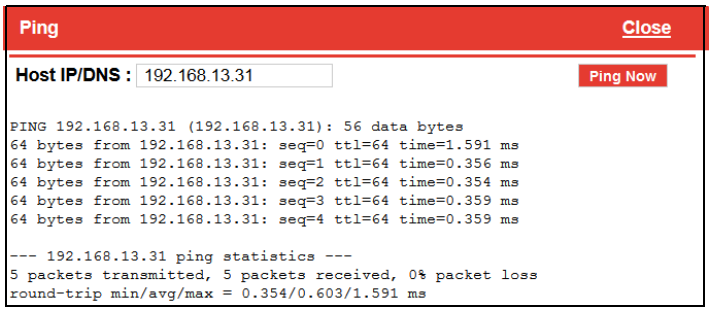
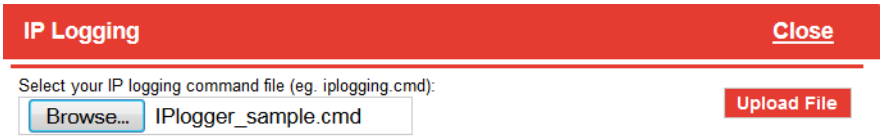
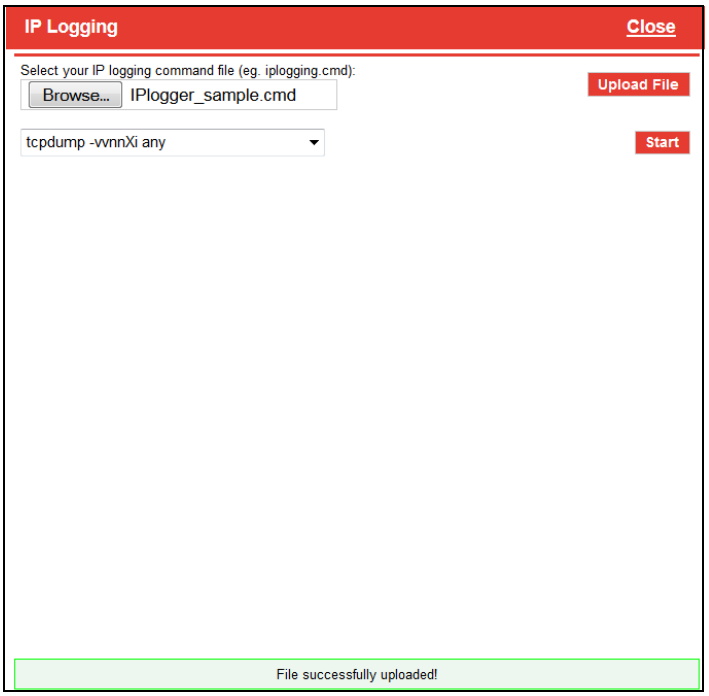
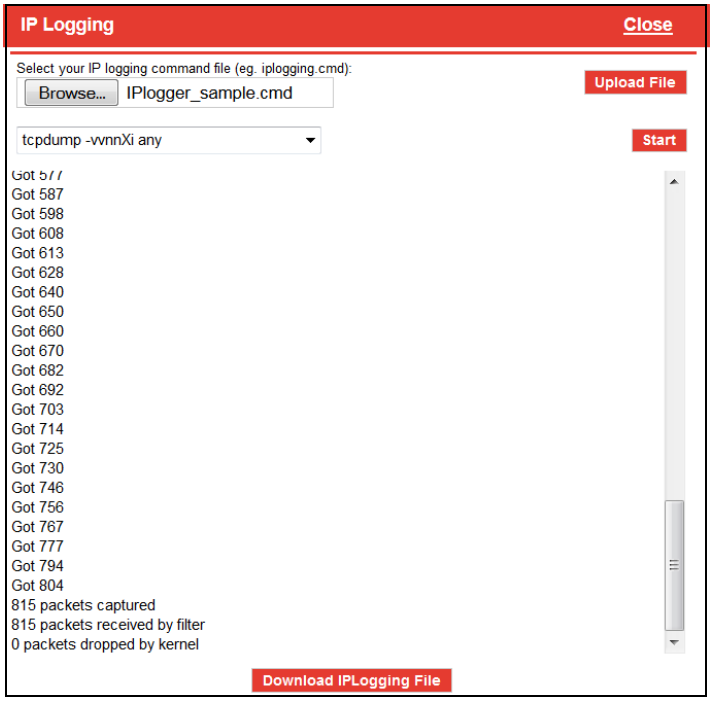


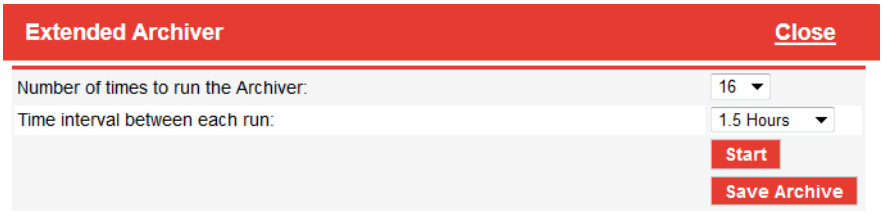
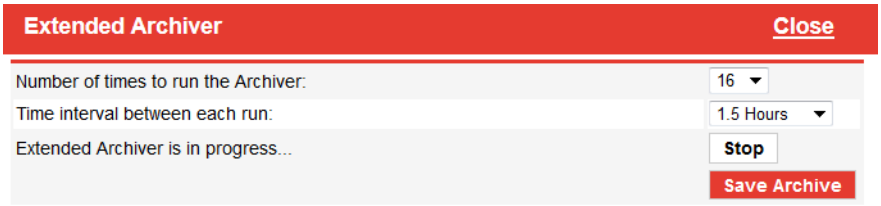
Figure 13-3: ACEmanager: Admin > Advanced

Field	Description
Date and Time	Queries the internal clock. The date and time are always specified in 24-hour notation (UTC). • mm/dd/yyyy=date in month/day/year notation • hh:mm:ss=time in 24-hour notation
Default Configuration Reset	Enables or disables the hardware reset button Sets the AirLink gateway to allow (or not allow) the hardware reset button to reset the device to the factory default settings. • Allowed—Pressing the hardware reset button for 7–10 seconds reboots the device and resets it to the factory defaults. (When resetting the device to factory default settings, release the reset when all four LEDs turn from red to yellow.) • Not Allowed—Pressing the hardware reset button reboots the device, but does **not** reset it to the factory defaults. *Note: This field only affects the **hardware** reset button on the device. You can always use the "Reset to Factory Defaults" button in ACEmanager to reset the device.* *Note: If this field is set to "Not Allowed" and the login password is subsequently lost, the only way to regain access to the AirLink gateway is through AirVantage Management Service (account required).*
Status Update Address	Enter the device Name/Port. Name is the domain name or IP address, and Port is the port of the device where the device status updates (in XML format) will be sent. This report can be sent to a LAN connected host (e.g., 192.168.13.100/1122) or a remote location (e.g., newb.eairlink.com/17000).
Status Update Period (seconds)	The time interval (in seconds) when a status update should be sent
Power Input Voltage (volts)	Displays the power input voltage in volts. If the input voltage ground is connected to the AirLink gateway case (without serial connection), this value reads .3 V (approx.) less; if ground is connected (with serial connection), the value reads .3 V (approx.) more.
Board Temperature (Celsius)	Displays the board temperature in degrees (Celsius)
Radio Module Internal Temperature (Celsius)	Displays the temperature of the internal radio module in degrees (Celsius).
Number of System Resets	Count of the number of system resets over the life of the device or since the last configuration reset
Periodic Reset Timer (hours)	Resets the device after the specified number of hours. 0 = Disabled
Time of Day (ToD) Reset: Reset Interval (days)	Number of days between resets 0 = Disabled Example: If this field is set to 3, the device resets every third day.

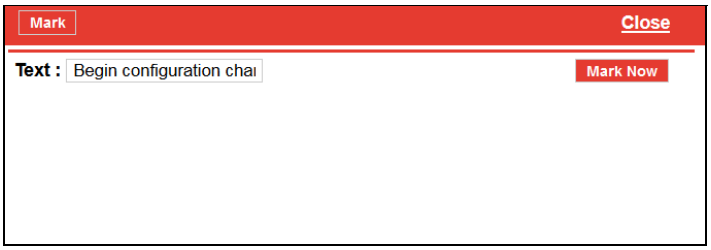
Field	Description
ToD Reset: Time Zone Offset from UTC	Time zone adjustment (Offset in easterly direction from UTC Time) Possible values are -12...12 Example: Pacific Standard Time would be -7
ToD Reset: Hour of day when Reset occurs	The local hour of the day when the reset occurs Possible values are 0–23 Example: 4 is 4:00 am
Minimum TLS Version	Sets the minimum TLS version that can be used for secure connections. By default (when set to TLS 1.0) the gateway makes outbound connection attempts using the most secure layer (TLS 1.2) and falls back to other layers if the remote host does not support it. When set to TLS 1.2, connection attempts using a lower version are blocked. Options are: • TLS 1.0 (default) • TLS 1.1 • TLS 1.2
Ping	Use this button to confirm that a connected device is responding. 1. Click Ping. 2. In the pop-up window, enter the device IP address or DNS name and click Ping Now. 

Field	Description
IP Logging	IP Logging is used to troubleshoot issues such as: • Problems with the LAN or WAN connection to an AirLink gateway • Uncertainty about where a packet is coming from • Issues with port forwarding not working properly IP Logging enables you to log network traffic and save it in a form that can be analyzed by Sierra Wireless engineers. Before using IP Logging, contact your authorized AirLink reseller or Sierra Wireless representative to discuss the issue you are observing and obtain a .cmd file to capture the appropriate related IP traffic. When you receive the file, save it to your computer's hard drive. To use IP logging: 1. Obtain a command (.cmd) file from Sierra Wireless. 2. In ACEmanager, go to Admin > Advanced and click IP Logging. 3. In the pop-up window, click Browse and navigate to the command file you received from Sierra Wireless. 4. Click Open. The file name appears in the field beside the Browse... button.  5. Click Upload File. 6. Once you see a message at the bottom of the window saying that the file has been successfully uploaded, select a command from the drop-down menu, as advised by your support contact.  7. Click the Start button.

Field	Description
IP Logging (continued)	*Note: If you are running more than one command, run each command sequentially and save the results before selecting the next command to run. Running a new command or re-running the same command wipes out the results from the previous run.* When the logging is complete, the log shows the number of packets captured, received, and dropped. *Note: If the log shows only "Got 0", no logs were captured. Contact Sierra Wireless.*  Once the logging is compete, click the Download IP Logging File button at the bottom of the screen, save the tarred gzip file (file extension .tgz) to your computer, and email it to your support contact.

Field	Description
Extended Archiver	Extended Archiver is a troubleshooting tool that enables you to collect logs covering an extended period of time. Before using it, contact your authorized AirLink reseller or Sierra Wireless representative to discuss the problem. To start the process: 1. Click Extended Archiver. 2. Select the following options, as advised by Sierra Wireless: • The number of times to run the archiver (1–25; default is 16) • The interval between runs (30 minutes, 1 hour, 1.5 hours, 2 hours, 2.5 hours, 3 hours, 3.5 hours, 4 hours, 4.5 hours, 5 hours, 5.5 hours, 6 hours, or 6.5 hours; default is 1.5 hours)  3. Click Start. The Extended Archiver saves the current set of logs. It waits for the configured interval and then collects another set of logs, which are saved to the same file. This process continues for the number of times the Archiver is configured to run. At any time, you can click Save Archive. The logs collected to that point are saved and the process continues.  4. Once the process is complete, click Save Archive, save the tarred gzip file (file extension .tgz) to your computer, and email it to your support contact. **Stopping and Restarting the Extended Archiver** After you click the Start button, it changes to Stop. To stop the process: 1. Click Save Archive if you want to save the logs already collected. 2. Click Stop. Logs not already saved will be lost. If desired, you can change the settings and restart the process. *Note: The Extended Archiver settings and the collected logs persist over reboots. Once the reboot is complete, the process resumes.*
Reset to Factory Default	Erases all customer-defined settings, including custom APNs and resets all settings (passwords, LAN and WAN configuration, security settings, ALEOS Applications Framework, etc.) to the original factory settings. AAF is also reset to disabled.

Field	Description
Reset Mode	Before resetting the AirLink gateway to the factory default settings, you can choose to preserve the configured network connection settings. Options are: • Reset All—All settings including network settings are returned to the factory default values on Reset to Factory Default. Note: Custom APNs on AirLink gateways with radio module MC7750 retain a custom APN after the reset to factory default settings. To change the APN, go to WAN > Cellular. To determine the type of radio module in your device, go to Status > About. • Preserve Cellular Authentication Settings—(default) When the device is returned to factory default settings (either by clicking the Reset to Factory Defaults button in ACEmanager, or pressing the hardware reset button as described in the Hardware User Guide), the following network settings are preserved: • Network User ID • Network Password • Network Authentication Mode • LTE Authentication Mode • APN Type • Select from the List (APN value) • User Entered APN • Backup APN • Backup Network Authentication Mode • Backup LTE Authentication Mode • Backup Network User ID • Backup Network Password • SIM Card PIN code • Status of the last PIN lock/unlock attempt • AVMS Enabled/Disabled status • AVMS Name (Device name in AVMS) • Device Initiated Interval (AVMS) • AVMS Server URL • HTTP Server and ACEview Services • M3DA Protocol Password • ACEmanager Remote Access • Reset Mode

Field	Description
Mark	This button is used to mark the start of a section in the device log and is typically used for troubleshooting. If asked to do so: 1. Click the Mark button and enter the text you want to appear in the log file. Alphanumeric characters, spaces, periods, commas, dashes, colons and semi-colons are allowed.  2. Click Mark Now. 3. Proceed with the configuration changes. 4. Generate a log file. (See Log on page 234.)
Diagnostic shell access	When enabled, this field allows Sierra Wireless TechSupport personnel to locally access the diagnostic shell on your gateway. It should be left at the default setting unless Sierra Wireless TechSupport asks you to change it.

Radio Passthru

Radio Passthru allows a direct connection, using USB, to the internal radio. Normal cellular radio operation is suspended while Radio Passthru is enabled.

Radio Passthru is generally used only in certain troubleshooting scenarios.

The hardware bypass will remain in effect until the ALEOS software resets either via ACEmanager command or the hardware Reset button.

Note: Because Radio Passthru is not USB/net or USB/serial, a different set of drivers are required to connect to the radio installed inside an AirLink gateway. Additionally, while it is possible to send AT commands to the radio using a terminal connection, there are software applications designed to communicate with the radio directly. If you need to use Radio Passthru, contact your Sierra Wireless AirLink representative to obtain the needed drivers and/or software application.

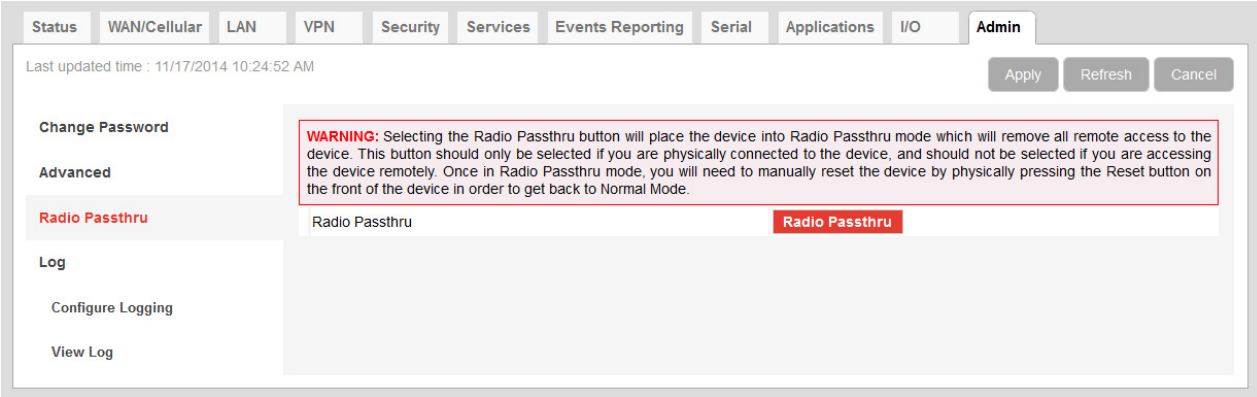


Figure 13-4: ACEmanager: Radio Passtrhru

Log

The Log file is a system log of the AirLink gateway.

The Logging configuration screen enables you to configure log verbosity and display filtering. The View Log screen enables you to view and save logs. The logs are in plain text.

To configure what you want to include in the logs:

1. In ACEmanager, go to Admin > Log.

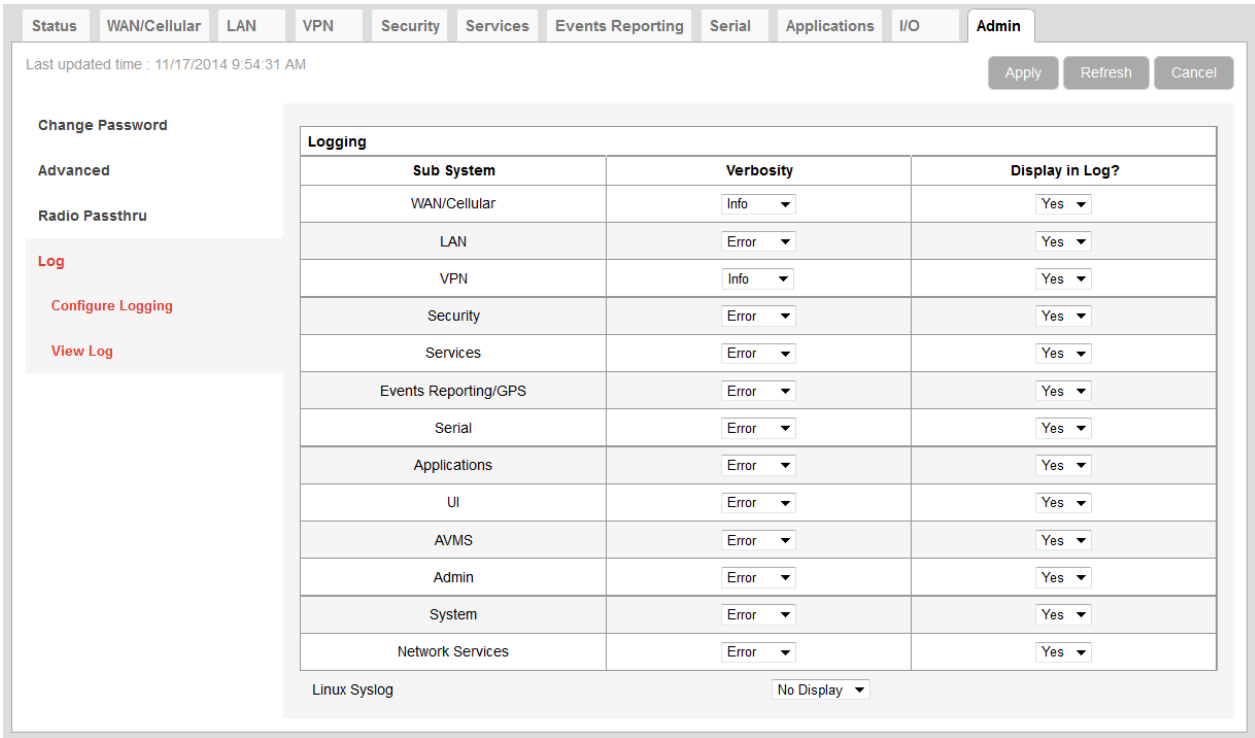


Figure 13-5: ACEmanager: Admin > Log, Configure Logging

2. For each subsystem listed:

a. Select whether or not to display it in the log.

Separate filters, based on subsystem and severity, are applied when the messages are generated and when the messages are displayed. Four severity levels are supported for filtering in the drop-down lists for verbosity:

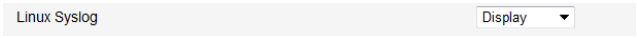
- Critical
- Error
- Info (information)
- Debug

Note: The VPN Sub System only allows for Info and Debug. For maximum information, set the VPN verbosity to Debug.

b. Select the verbosity level.

Note: Some log messages are only displayed if you display Linux Syslog. For example, If you are debugging a VPN or LAN setup, the relevant information is only displayed in the Linux Syslog.

3. Optional: To display Linux Syslog:
   a. Ensure that Display (default value) is selected the drop-down menu beside Linux Syslog.



4. Click Apply.
5. If you have changed any of the verbosity levels or the Linux syslog setting:
   a. Reboot the AirLink gateway.
   b. Log into ACEmanager, go to Admin > Log.
6. Select View Logs from the menu on the left side of the page.

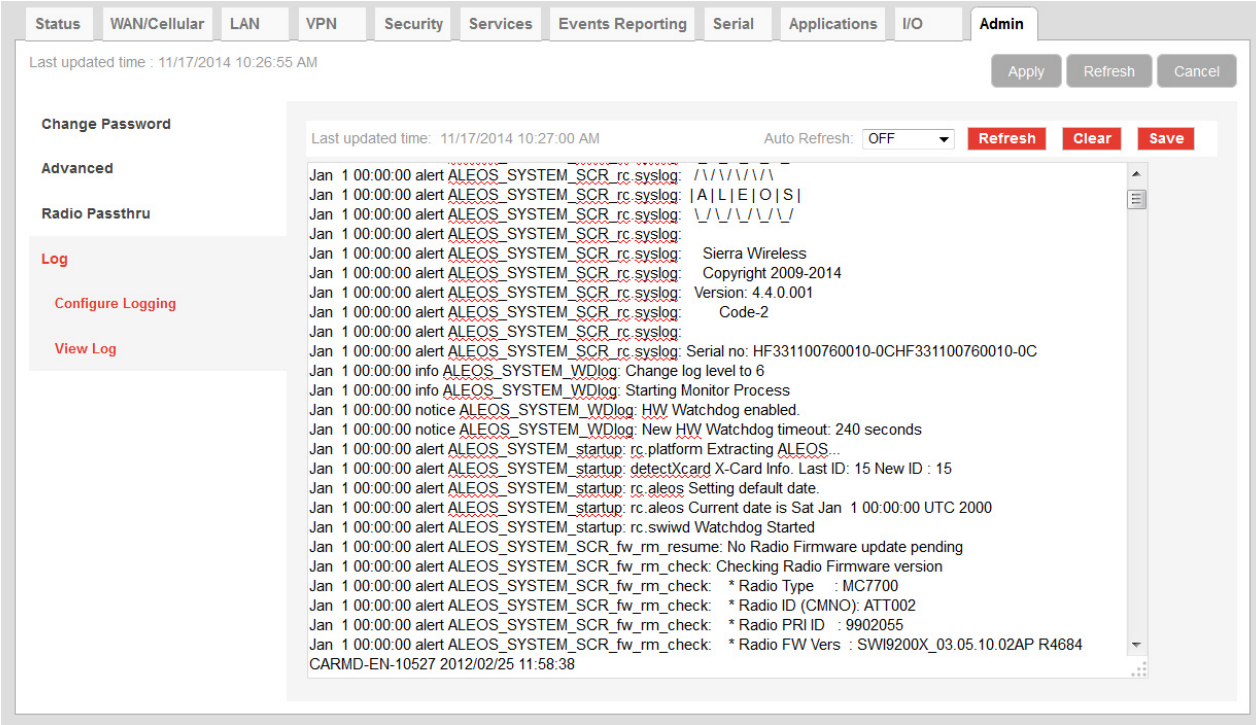


Figure 13-6: ACEmanager: Admin > Log, View Log

Note: VPN info and debug information uses the term racoon (rather than VPN), as shown in Figure 13-6.

Note: If you toggle the "Display in Log?" field, clear and refresh the View Log page. (You do not need to reboot the device.)

Tip: *Use View Log for troubleshooting purposes (e.g., when setting up the IPsec configuration). The Log page allows you to establish the tunnel connection and monitor the results directly. To change the intervals at which the log is displayed, you can change the settings in Auto Refresh.*

Actions on the View Log screen include:

- Auto Refresh — The drop-down menu allows you to set up an automatic log page refresh, and the interval between refreshes: 30 secs, 1 minute, or 2 minutes.
- Refresh button — Initiates a manual page refresh
- Clear button — Clears out the tunnels
- Save button — Creates a text file of the log

A: Windows Dial-up Networking (DUN)

Dial-up Networking (DUN) enables you to use Point-to-Point Protocol (PPP) to establish a connection between a host PC serial port and the AirLink gateway, as shown in Figure A-1.

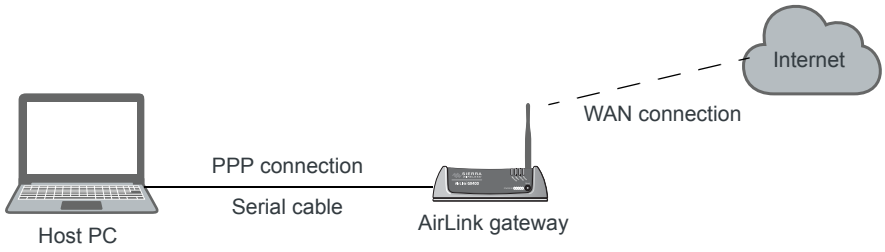


Figure A-1: PPP connection

Caution: *To install any driver on your computer, you may need to be logged in as Administrator or have Administrator privileges for your login.*

Microsoft Windows 7 is used in the examples below. The device driver installation and DUN setup and configuration is similar in other Microsoft Windows operating systems, including Windows XP and Windows CE.

Note: If your device is new, or has recently been reset to factory default settings, ensure that the device has been on air at least once before being used with a DUN connection.

Installing a Device Driver

Connect the AirLink gateway

1. Connect the device to the computer with a DB-9 cable from one RS-232 port to the other.
2. Log in to ACEmanager.
3. Go to Serial > Port Configuration.
4. Set the DB9 Serial Echo field to Disable.
5. Reboot.

Note: You need to set the DB9 Serial Echo field echo to Disable any time you want to set up a PPP connection.

Install the driver

1. Select Start > Control Panel > Phone and Modem Options.

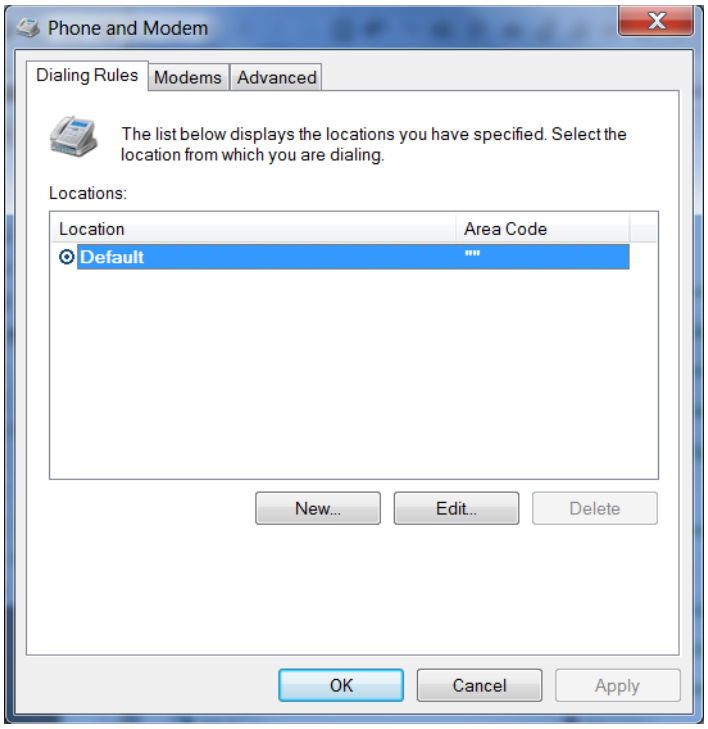


Figure A-2: Phone and Modem Options

2. Select the Modems tab.

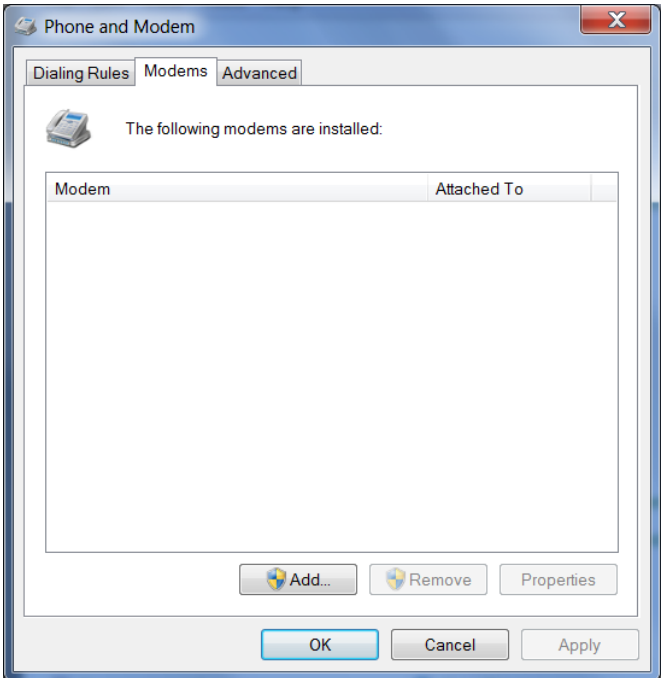


Figure A-3: Phone and Modem Options: devices

3. Click Add.

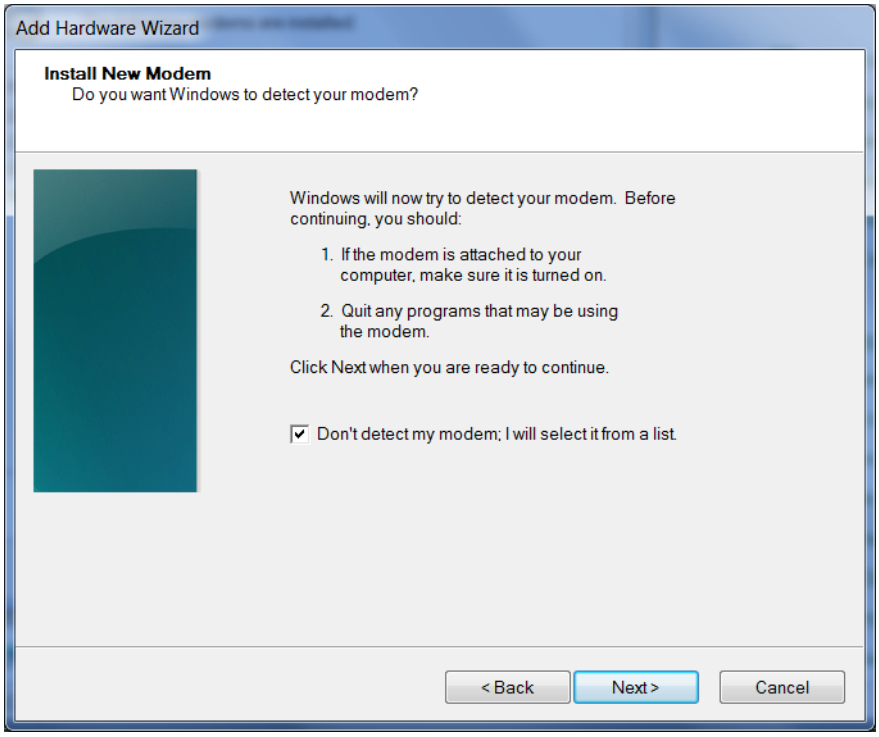


Figure A-4: Add Hardware Wizard

4. Select Don't detect my modem; I will select it from a list.
5. Click Next.

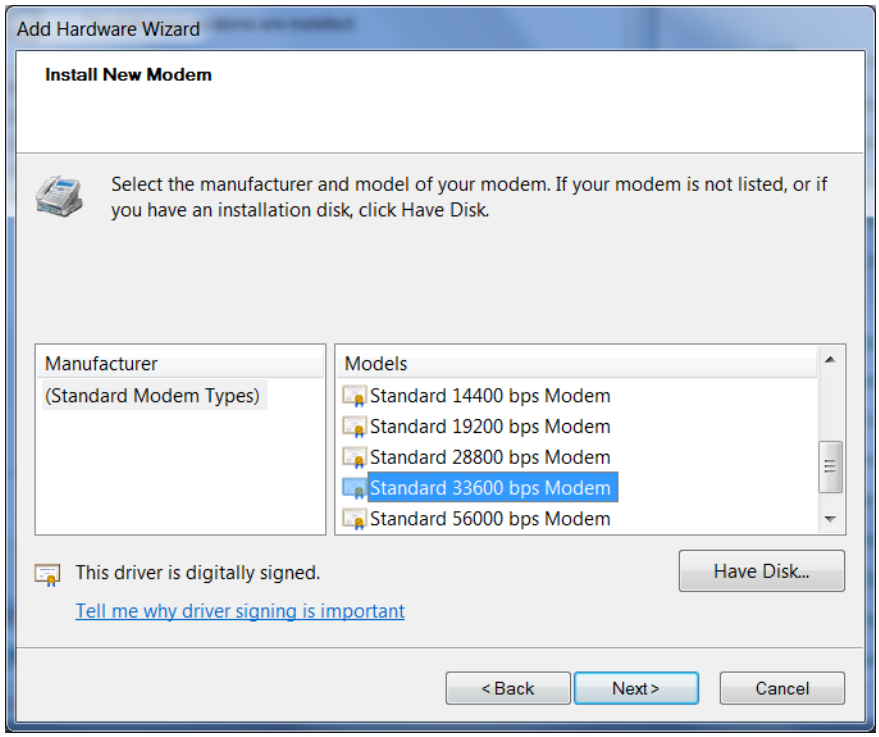


Figure A-5: Add Hardware Wizard: Install New Modem

6. Under Manufacturer, select (Standard Modem Types).
7. Under Models, select Standard 33600 bps Modem.

Tip: *If you have the speed for your device configured as something other than the default, use the Standard device that matches the speed you configured.*

8. Click Next.

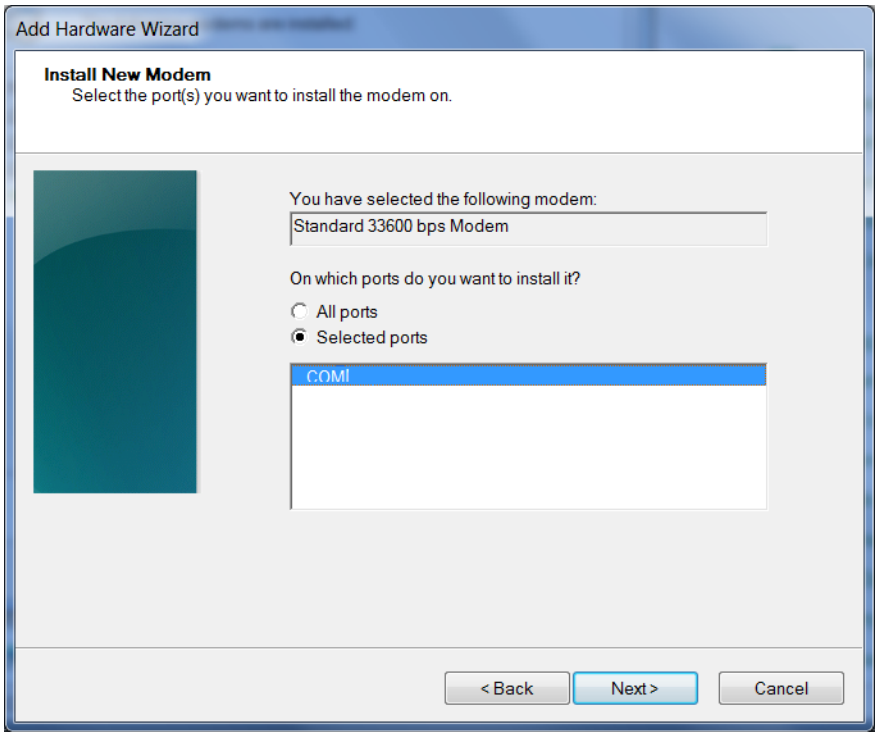


Figure A-6: Add Hardware Wizard: Select Ports

9. Select Selected Ports.
10. Select the COM port the device is connected to (commonly COM1).
11. Click Next.

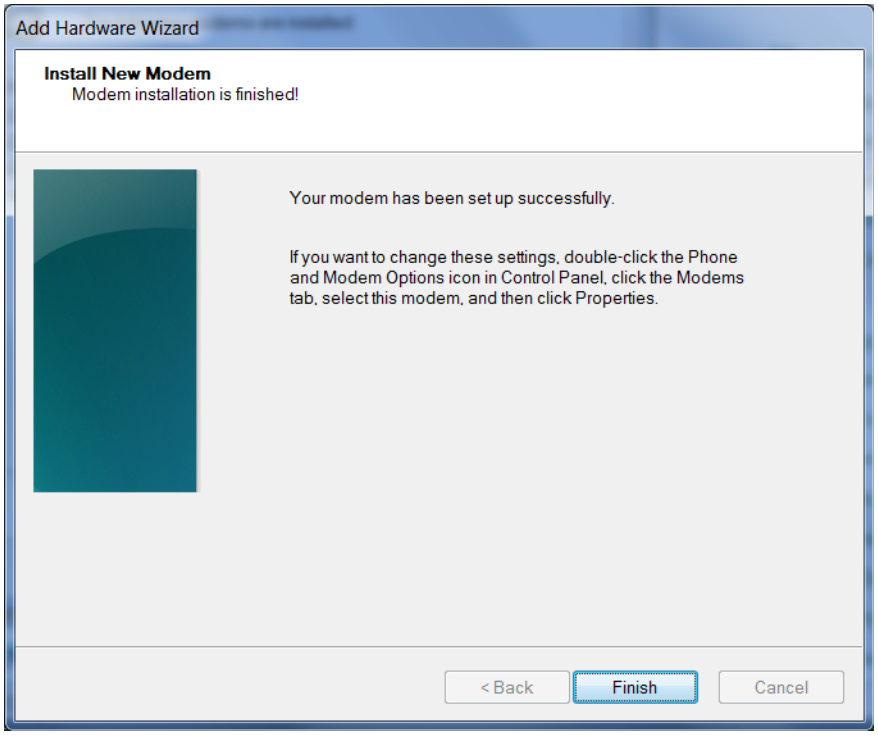


Figure A-7: Add Hardware Wizard: Finish

12. Once the device driver is installed, click Finish.

When you return to the Phone and Modem Options page, you should see the newly installed device “attached to” the correct COM port.

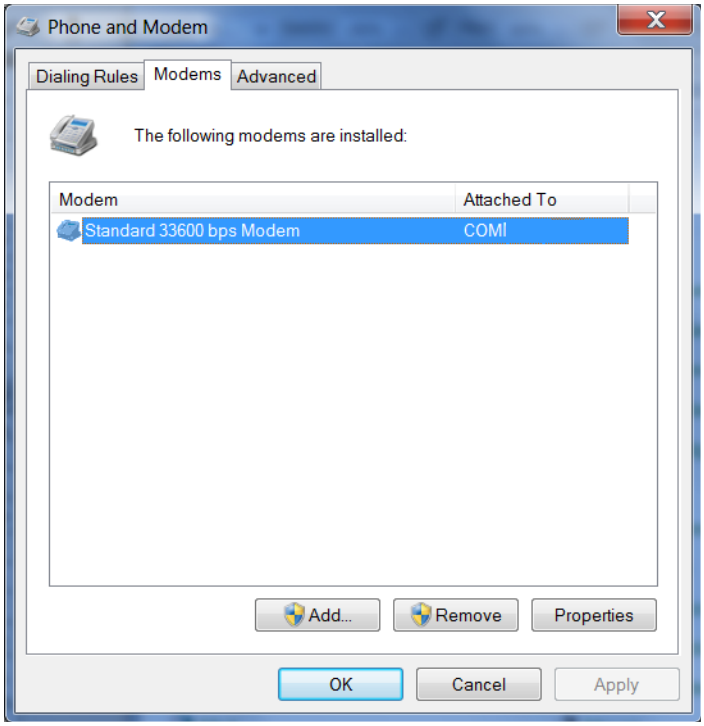


Figure A-8: Phone and Modem Options > Modems

13. Highlight the modem, and click Properties. The following window appears:

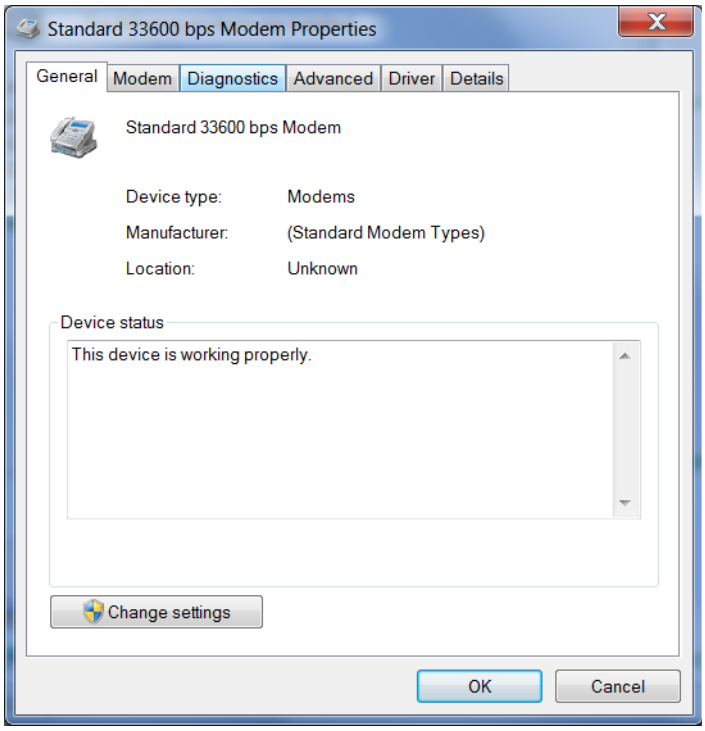


Figure A-9: Modem Properties

14. Select the Modem tab.

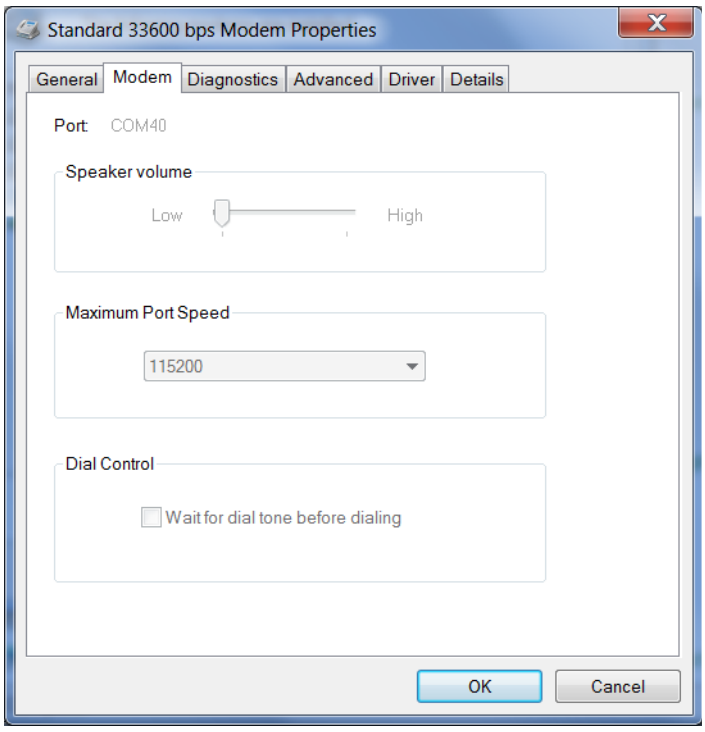


Figure A-10: Modem Properties > Modem

15. Confirm that the Maximum Port Speed is set to 115200 (default).

16. Click OK to exit.
17. Click OK again to exit out of the Phone and Modem Options.
18. Go to Start > Control Panel > Device Manager.

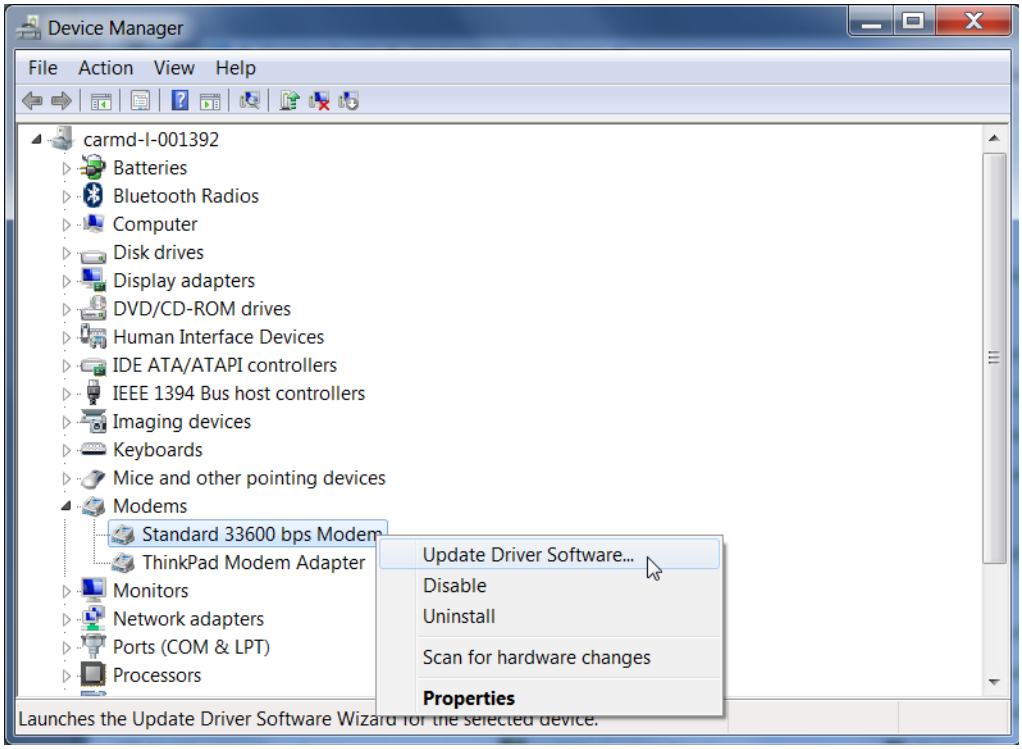


Figure A-11: Device Manager

19. Under Modems, highlight Standard 33600 bps Modem. Right-click and select Update Driver Software....

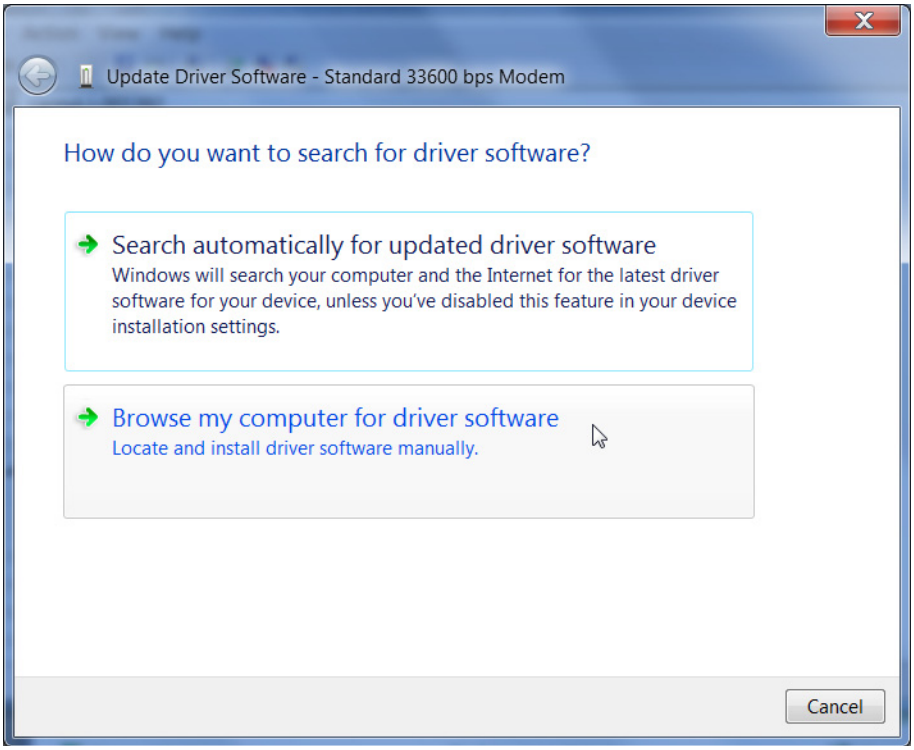


Figure A-12: Update Driver Software—Browse

20. Select Browse my computer for driver software.

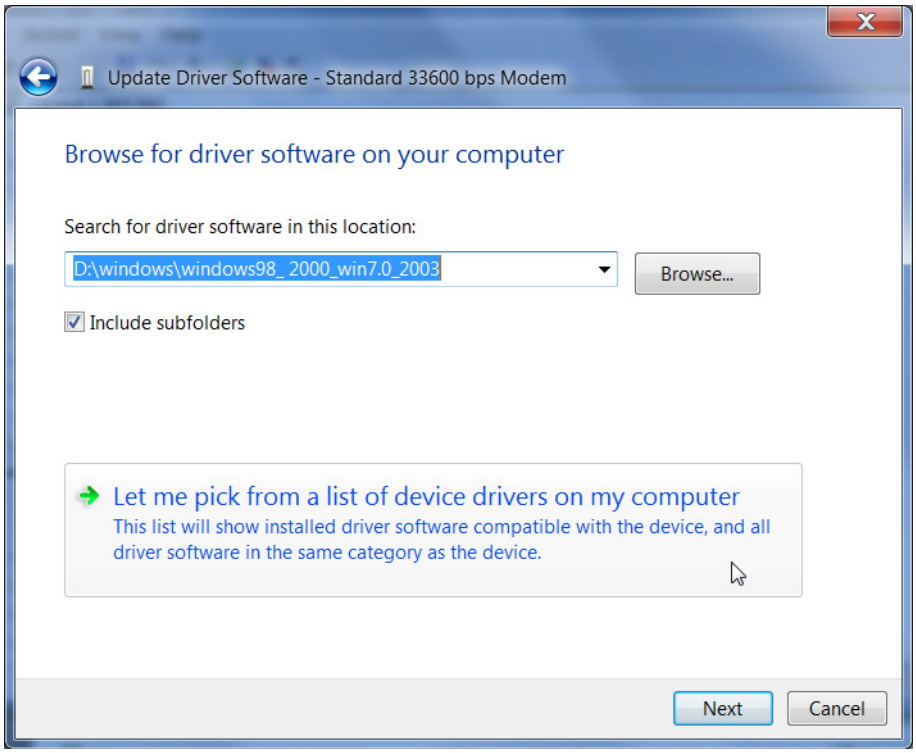


Figure A-13: Update Driver Software—Let me pick...

21. Select Let me pick from a list of device drivers on my computer.

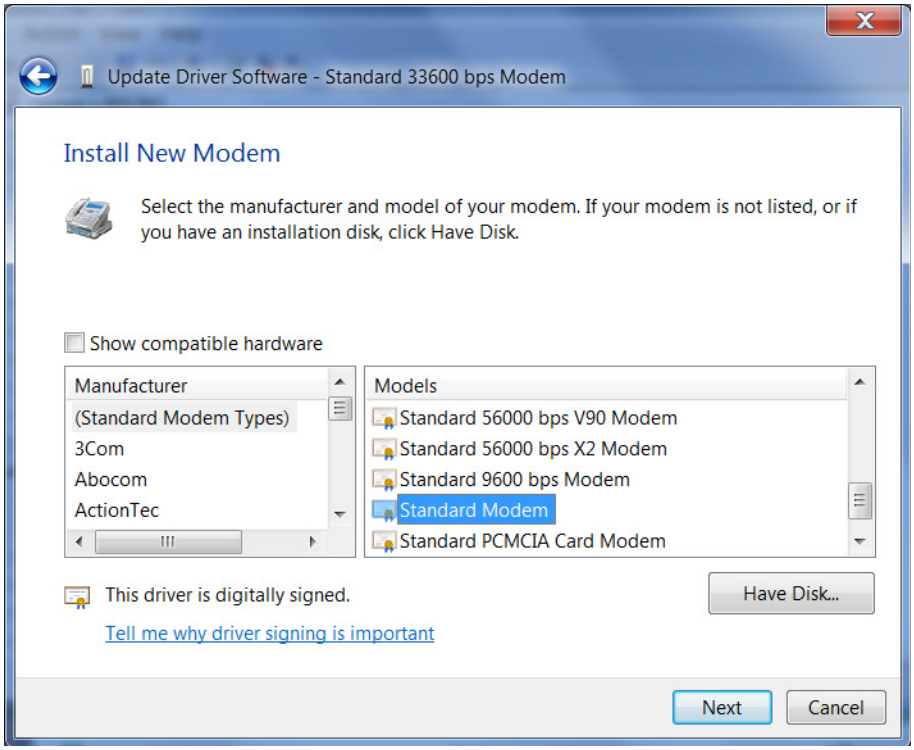


Figure A-14: Update Driver Software—Select Standard Modem

22. Deselect Show compatible hardware.
23. Under Manufacturer, select (Standard Modem Types).
24. Under Models, select Standard Modem.
25. Click Next.

    If you see an Update Driver Warning, click Yes.

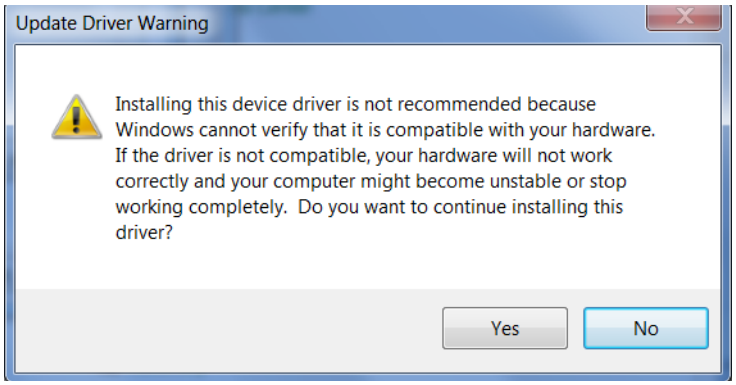


Figure A-15: Update Driver Software—Warning

The software driver updates and the following window appears:

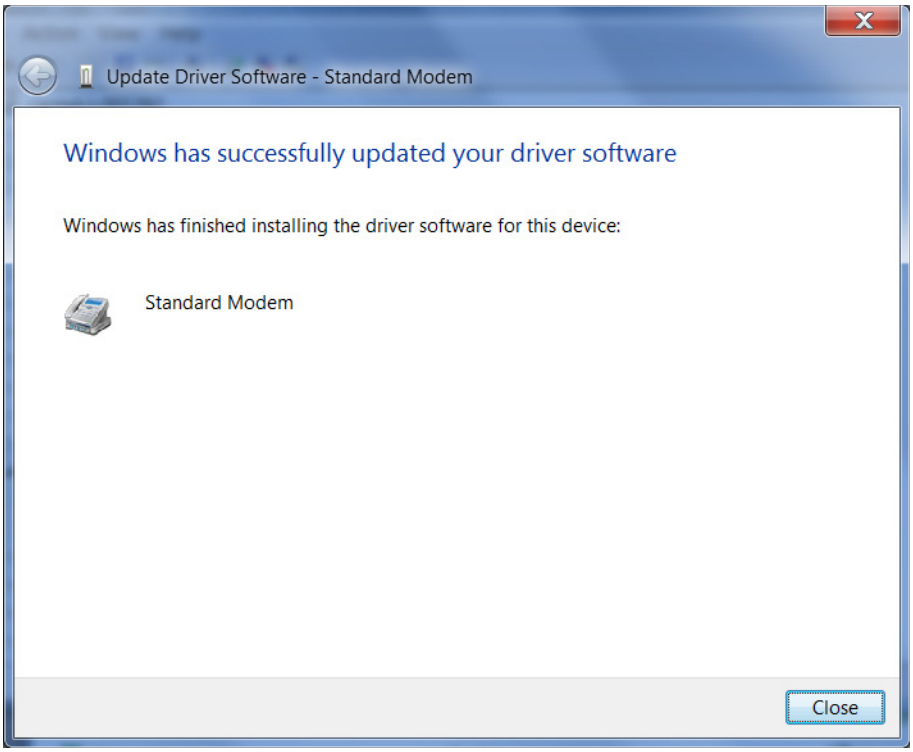


Figure A-16: Update Driver Software—Success

26. Click Close.

Creating a Dial-Up Networking (PPP) Connection

Once you have the driver for the modem installed on your computer, you can set up and configure Dial Up Networking (DUN).

Note: No other device or program can use the COM port (serial port) configured for the modem driver while the DUN session is active.

Caution: *If you have an existing LAN connection, installing DUN for the AirLink gateway may interfere with the LAN connection. We recommend disconnecting your LAN connection before using a PPP connection with your AirLink gateway.*

Once you have configured the DUN connection on your computer:

- The DUN connection may be set as the default connection.
- The computer may be configured to dial the DUN connection when it cannot detect any network connection.

For instructions on changing these options, see Connection settings on page 255.

If you are using a DUN connection with any other network connection (such as Ethernet), you may need to use the route command in Windows to set up a static route through the device to access the location remotely over the PPP link and the mobile network. This guide does not provide information on the route command. Consult your network administrator for information on properly configuring routing.

Create a new network connection.

1. Select Start > Control Panel > Network and Sharing Center.

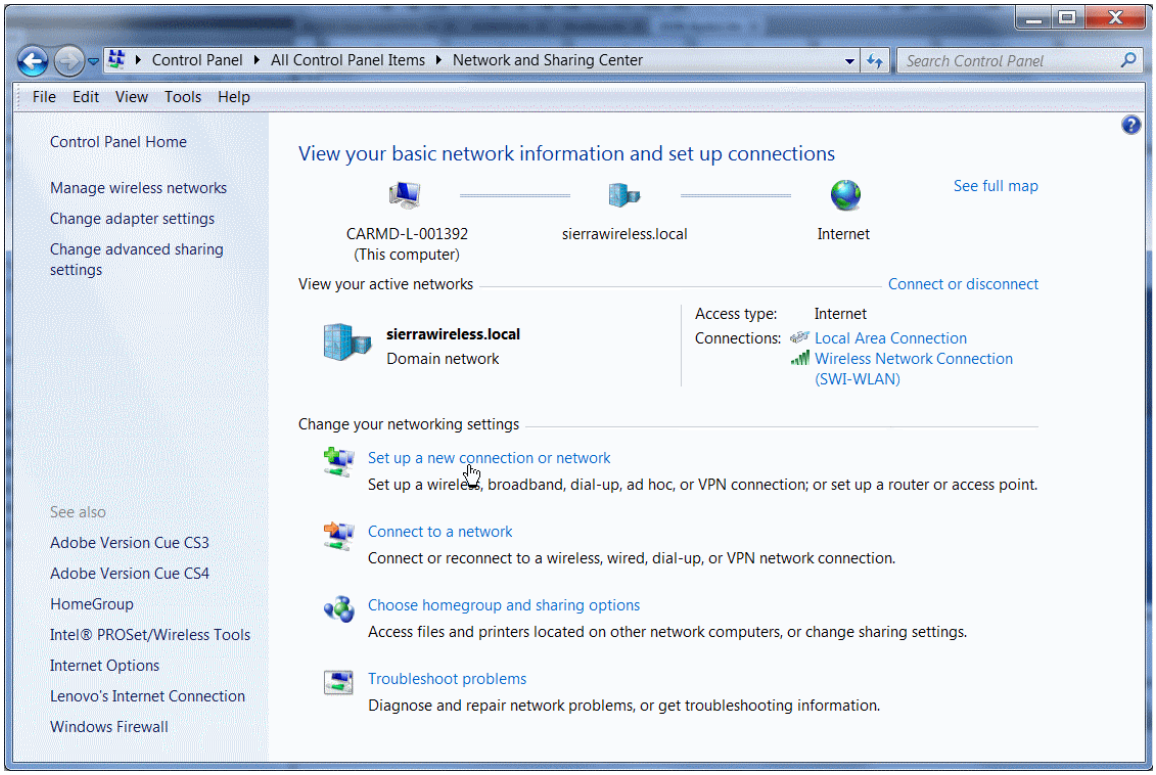


Figure A-17: Network and Sharing Center Window

2. Select Set up a new connection or network.

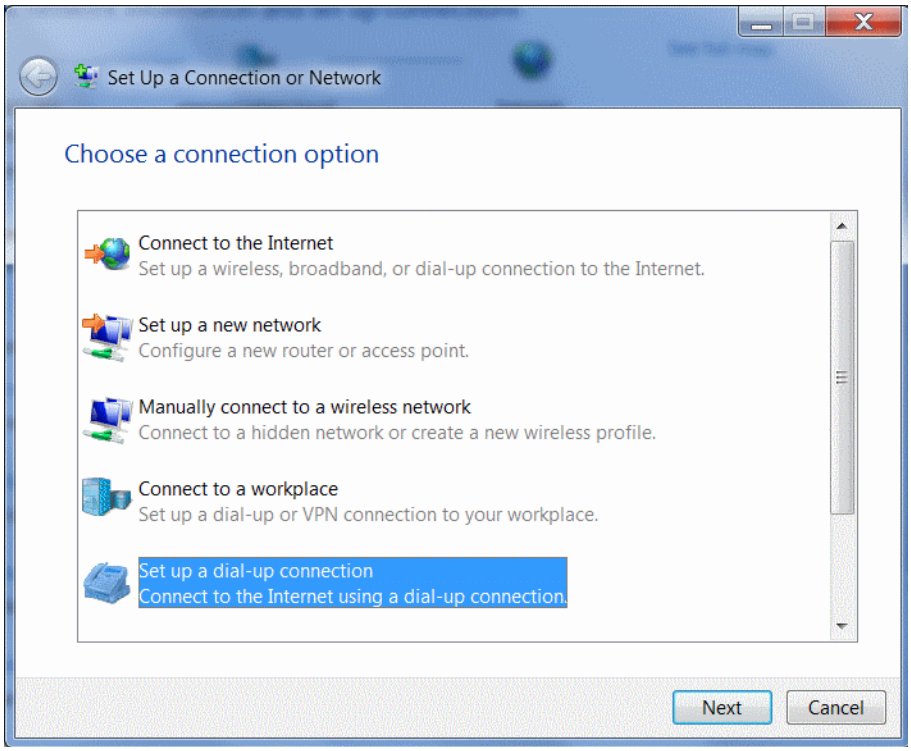


Figure A-18: Set up a Connection or Network

3. Select Set up a dial-up connection.
4. Click Next.

   If you are asked which modem you want to use, select Standard Modem.

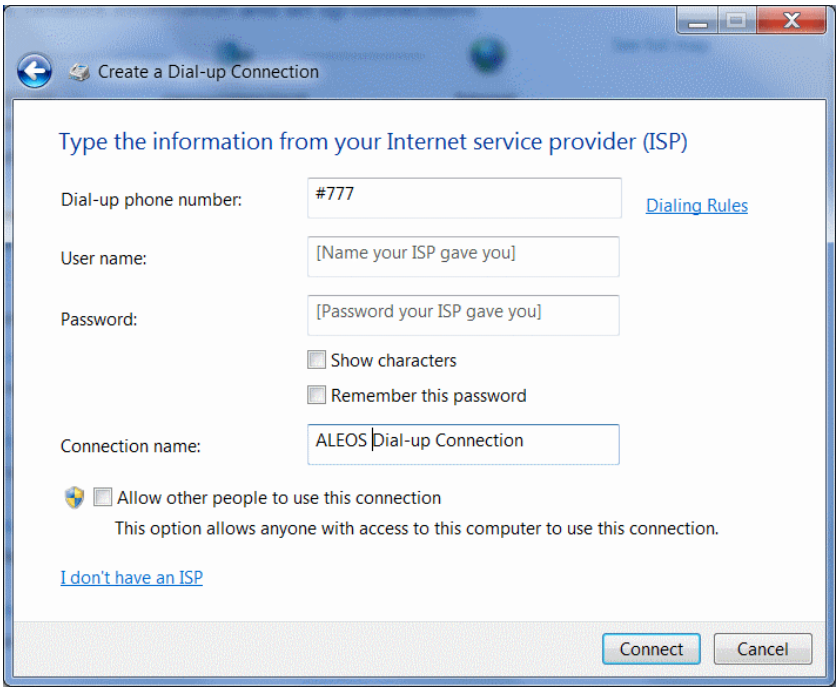


Figure A-19: Create a Dial up Connection

5. In the Dial-up phone number field, type “#777”.
6. Ignore the User name and Password fields.
7. In the Connection name field, type “ALEOS Dial-up Connection” or other desired name.
8. Click Connect.

   Alternatively, to connect to the ALEOS Dial-up network:

   a. Click the network connection icon[1] in the system tray.
   b. Select ALEOS Dial-up Connection.
   c. Click Connect.

Configure the DUN connection

After you complete the New Connection Wizard:

1. Click the network connection icon, select ALEOS Dial-up Connection, and click Connect.

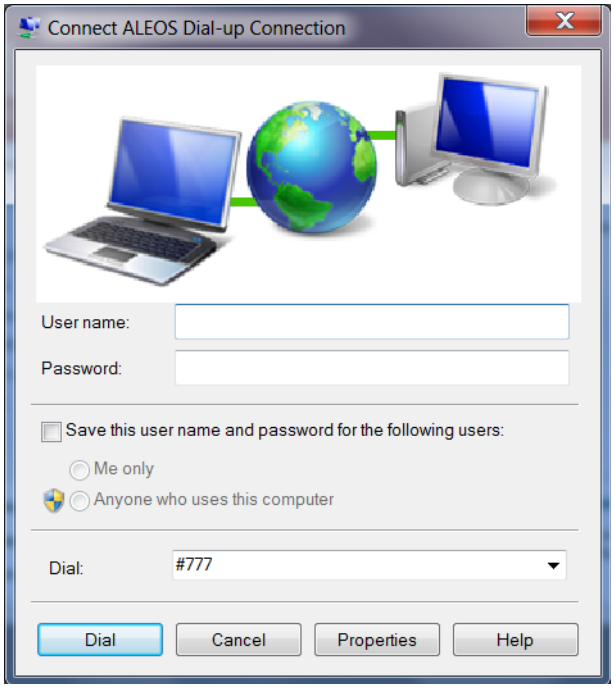


Figure A-20: DUN Connection

2. If you have a user name and password configured in ACEmanager for PPP connections, enter them in the User name and Password fields. Otherwise, leave these fields blank.
3. Click Properties.

1. The appearance of the connection icon varies depending on the type of connections available. For example, It may appear as , , or .

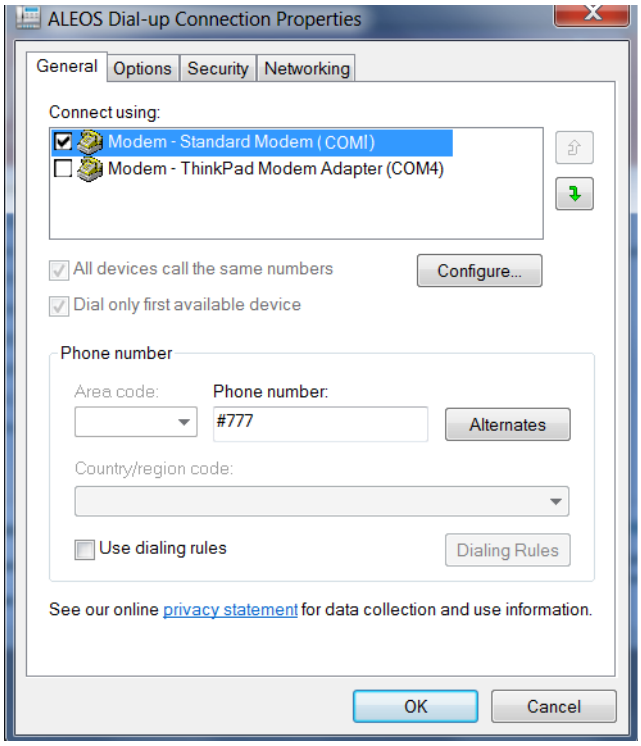


Figure A-21: DUN Properties

4. Confirm that the check box beside Use dialing rules is not selected.
5. Click Configure... (below the Connect using box).

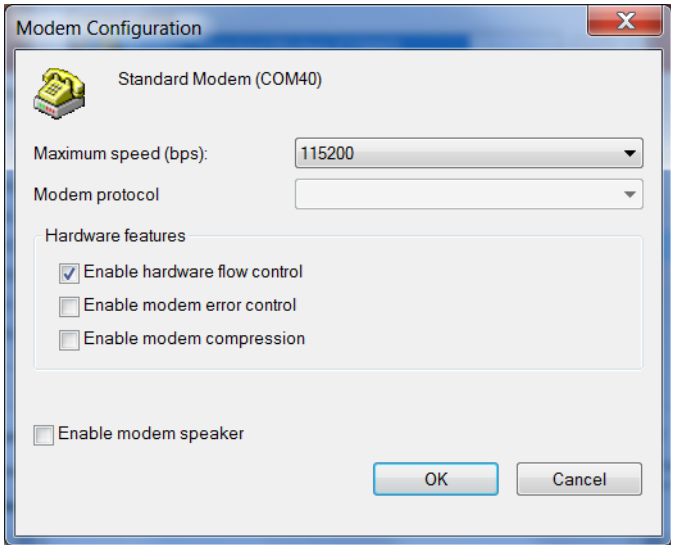


Figure A-22: Modem Configuration

6. Confirm that the Maximum speed (bps) is set to 115200.
7. Confirm that Enable hardware flow control is selected. Do not select any other options.
8. Click OK.

9. In the main properties window, select the Options tab.

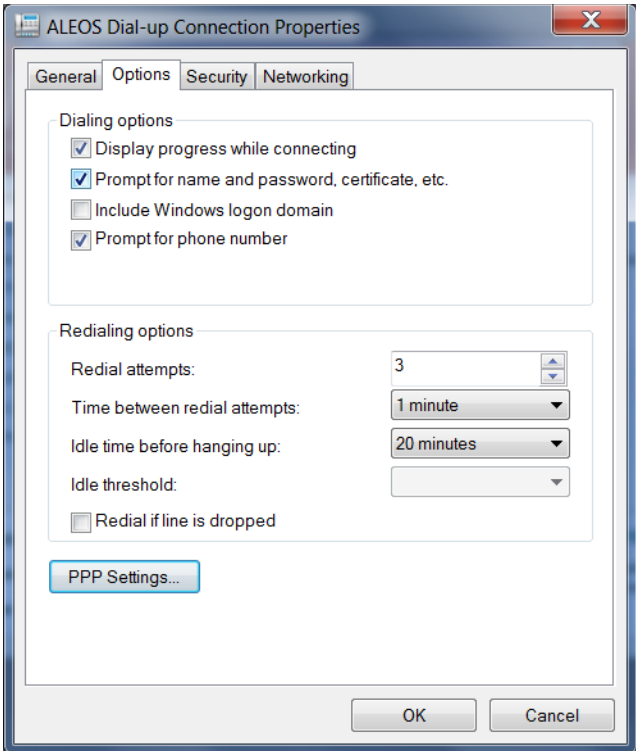


Figure A-23: Networking

10. Click PPP Settings.

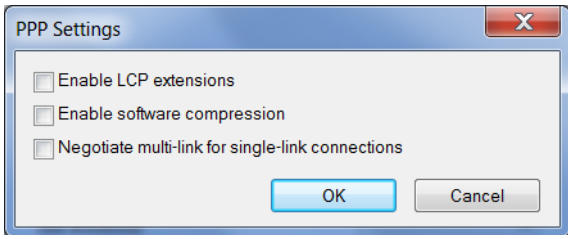


Figure A-24: PPP Settings

11. Clear the check boxes beside all three PPP settings.
12. Click OK.
13. Select the Networking tab.

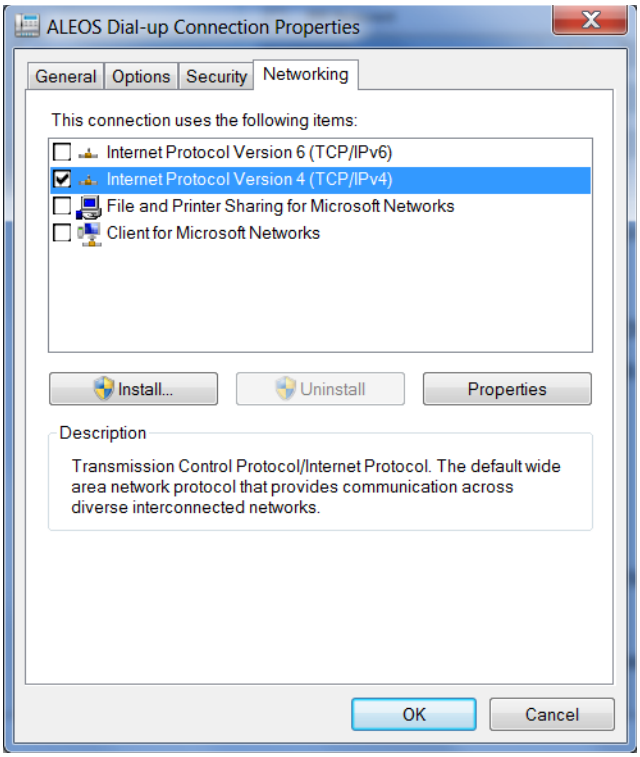


Figure A-25: DUN Connection > Networking tab

14. Select Internet Protocol Version 4 (TCP/IPv4) and then select Properties.

Tip: *For most configurations, getting the IP address and the DNS server address are automatic.*

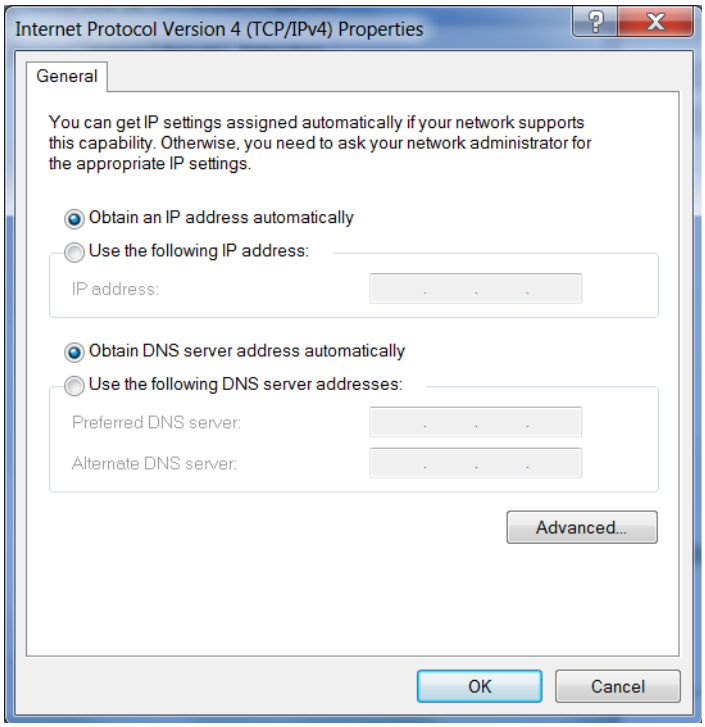


Figure A-26: TCP/IP Properties

15. Click Advanced.

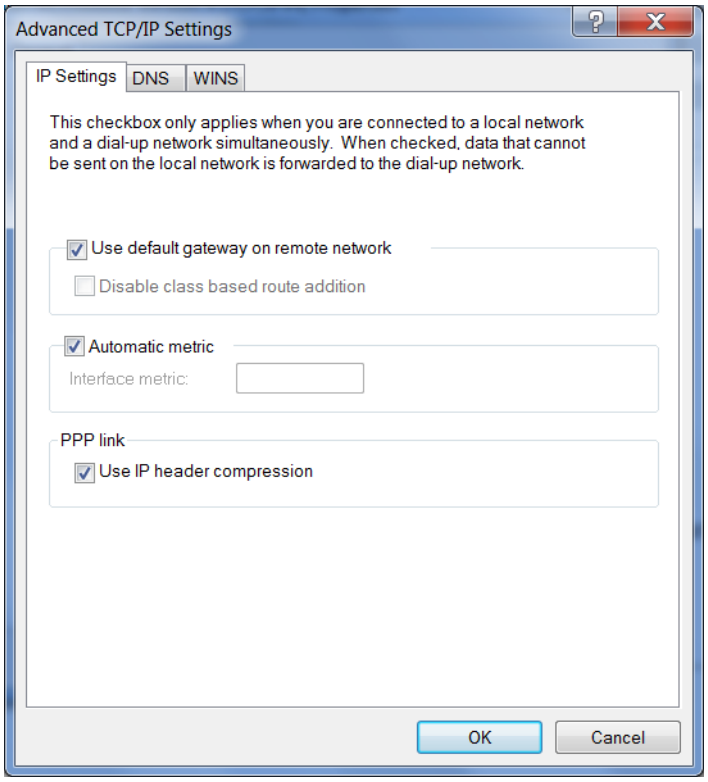


Figure A-27: Advanced TCP/IP

16. Select Use default gateway on remote network.
17. Click OK.

Tip: *You may want to check the Options tab and change the settings for applications you use. The default options are generally applicable for most uses.*

Caution: *Unless specifically directed to do so by Support or your network administrator, you do not need to make any changes to the options on the Security tab.*

18. Click OK until you return to the Connect window.
19. Log in to ACEmanager and go to Serial > Port Configuration.

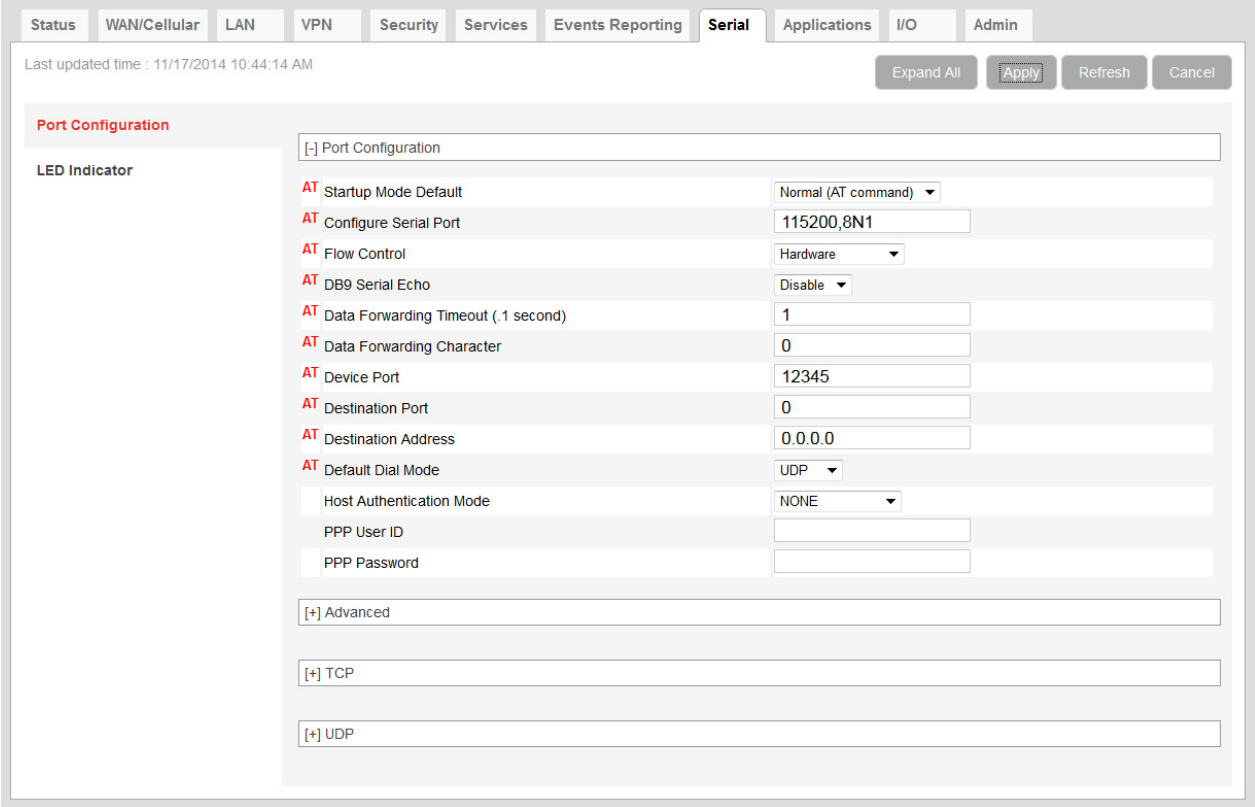


Figure 1-28: ACEmanager: Serial > Port Configuration

20. Under Port Configuration:
    a. Set the Flow Control field to Hardware.
    b. Set the DB9 Serial Echo field to Disable.
21. Click Apply and reboot the device.

Connection settings

1. To set the default connection:
2. Go to Start > Control Panel > Network and Sharing Center.

3. Select Change adapter settings.
4. Right-click the icon for the DUN connection.

   If you want this to be your default connection, select Set as Default Connection.

   If it is already the default connection and you do not want it as your default connection, select Cancel as Default Connection.

If you do not want the DUN connection to be dialed when there is no other connection:

1. Go to Start > Control Panel > Internet Options.
2. Select the Connections tab.
3. Highlight the DUN connection and select Never dial a connection.
4. Click Apply.
5. Click OK.

B: SNMP: Simple Network Management Protocol

Management Information Base (MIB)

ALEOS includes a Management Information Base (MIB) that contains information specific to the AirLink gateway. Reports based on this database are sent in a form designed to be parsed by the NMS. The data is hierarchical with entries addressed through object identifiers.

The MIB complies with:

- RFC 1213 and MIB-II
- RFC 2665 — Ethernet-Like Interface Types
- RFC 2863 — The Interfaces Group MIB

SNMP Traps

SNMP traps are alerts that can be sent from the managed device to the Network Management System when an event happens. Your AirLink gateway is capable of sending traps when the network connection becomes available.

To send SNMP traps:

1. In ACEmanager, go to Services > Management (SNMP).
2. Configure the fields under Trap Server User. (For more information, see Management (SNMP) on page 172.)
3. Go to Events Reporting > Actions.
4. In the Action Type field select SNMP trap. (For more information, see SNMP TRAP on page 187.)
5. Go Events Reporting > Events and configure monitoring for the event type that will trigger the SNMP trap. For example, the event type could be RSSI, thresholds, network state, hardware temperature, etc.

Sierra Wireless MIB

This section show the contents of the Sierra Wireless MIB file. When this file is loaded onto a remote SNMP client, you can query the Sierra Wireless specific objects listed in this file.

For a text copy of this MIB file, go to source.sierrawireless.com, and select your AirLink gateway.

Note: Some MIB elements such as GPS do not apply to the ES Series gateways.

```
SIERRA-MIB DEFINITIONS ::= BEGIN

IMPORTS
   OBJECT-TYPE, NOTIFICATION-TYPE, MODULE-IDENTITY, IpAddress,
   Integer32, Opaque, enterprises, Counter32, Unsigned32
```

```
        FROM SNMPv2-SMI

    TEXTUAL-CONVENTION, DisplayString, TruthValue
FROM SNMPv2-TC;

sierrawireless MODULE-IDENTITY
    LAST-UPDATED "201202290000Z"
    ORGANIZATION "Sierra Wireless Inc"
    CONTACT-INFO
"Sierra Wirelss Inc
        "

    DESCRIPTION
""
    REVISION "201202290000Z"

    DESCRIPTION
"This file defines the private Sierra MIB extensions."

    ::= { enterprises 20542 }

sharks OBJECT IDENTIFIER ::= { sierrawireless  9}

-- MIB versions

mibversion1 OBJECT IDENTIFIER ::= { sharks  1}

--  GUI Tabs for Sharks

statustab OBJECT IDENTIFIER ::= { mibversion1  1}
cellulartab OBJECT IDENTIFIER ::= { mibversion1  2}
lantab OBJECT IDENTIFIER ::= { mibversion1  3}
vpntab OBJECT IDENTIFIER ::= { mibversion1 4}
securitytab OBJECT IDENTIFIER ::= { mibversion1  5}
servicestab OBJECT IDENTIFIER ::= { mibversion1  6}
gpstab OBJECT IDENTIFIER ::= { mibversion1  7}
eventsreportingtab OBJECT IDENTIFIER ::= { mibversion1  8}
serialtab OBJECT IDENTIFIER ::= { mibversion1  9}
iotab OBJECT IDENTIFIER ::= { mibversion1  10}
admintab OBJECT IDENTIFIER ::= { mibversion1  11}
snmpconfig OBJECT IDENTIFIER ::= { mibversion1  12}

--  status elements

home   OBJECT IDENTIFIER ::= { statustab  1}
cellular OBJECT IDENTIFIER ::= { statustab  2}
lan  OBJECT IDENTIFIER ::= { statustab  3}
vpn     OBJECT IDENTIFIER ::= { statustab  4}
security     OBJECT IDENTIFIER ::= { statustab  5}
services     OBJECT IDENTIFIER ::= { statustab  6}
gps     OBJECT IDENTIFIER ::= { statustab  7}
serial     OBJECT IDENTIFIER ::= { statustab  8}
```

```
about     OBJECT IDENTIFIER ::= { statustab  9}


--  home status elements

phoneNumber OBJECT-TYPE
SYNTAX DisplayString (SIZE (10))
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 17 }

ipAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 301 }

networkState OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 259 }

rssi OBJECT-TYPE
SYNTAX INTEGER(-125..-50)
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 261 }

gprsnetworkOperator OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 770 }

cdmanetworkOperator OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 644 }

gprsECIO OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
 DESCRIPTION ""
```

```
::= { home 772 }

cdmaECIO OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
  DESCRIPTION ""
::= { home 643 }

powerIn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 266 }

boardTemprature OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 267 }

networkServiceType OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 264}

aleosSWVer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 4 }

netChannel OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 260 }

cellularBytesSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 283 }

cellularBytesRecvd OBJECT-TYPE
```

```
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 284 }


deviceName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { home 1154 }

--  cellular status elements

wanIP OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 301 }

electronicID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 10 }

iccid OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 771 }

cellid OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 773 }

lac OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 774 }

imsi OBJECT-TYPE
```

```
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 785 }

keepAliveIpAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1105 }

keepAlivePingTime OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1104 }

dnsServer1 OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1082 }

dnsServer2 OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 1083 }

cellBand OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 2056 }

apn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 2151 }

wanUseTime OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
```

```
   DESCRIPTION ""
::= { cellular 5046 }

rscp OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 10249 }

errorRate OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 263 }

bytesSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 283 }

bytesRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 284 }

packetsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 281 }

packetsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 282 }

prlVersion OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 642 }
```

```
prlUpdateStatus OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 646 }

sid OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 648 }

nid OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 649 }

pnOffset OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 650 }

baseClass OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { cellular 651 }

--  LAN status elements

usbMode OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 1130 }

vrrpEnabled OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { lan 9001 }

lanpacketsSent OBJECT-TYPE
```

SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
DESCRIPTION ""
::= { lan 279 }

lanpacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
DESCRIPTION ""
::= { lan 280 }

wifipacketsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
DESCRIPTION ""
::= { lan 10405 }

wifipacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
DESCRIPTION ""
::= { lan 10406 }

wifiBridgeEnabled OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION ""
::= { lan 10401 }

wifiSecurityType OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION ""
::= { lan 4509 }

wifiAPStatus OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
DESCRIPTION ""
::= { lan 4506 }

wifiSSID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current

```
    DESCRIPTION ""
::= { lan 4507 }

wifiChannel OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
    DESCRIPTION ""
::= { lan 4508 }

--  VPN status elements


incomingOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
    DESCRIPTION ""
::= { vpn 3177 }

outgoingOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
    DESCRIPTION ""
::= { vpn 3178 }

outgoingHostOOB OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
    DESCRIPTION ""
::= { vpn 3179 }


vpn1Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
    DESCRIPTION ""
::= { vpn 3176 }

vpn2Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
    DESCRIPTION ""
::= { vpn 3205 }

vpn3Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
```

```
STATUS current
   DESCRIPTION ""
::= { vpn 3231 }

vpn4Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3257 }

vpn5Status OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { vpn 3283 }

--  Security status elements

dmz OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 5113 }

portForwarding OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 5112 }

portFilteringIn OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 3505 }

portFilteringOut OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 3506 }

trustedHosts OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
```

```
   DESCRIPTION ""
::= { security 1062 }

macFiltering OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 3509 }

badPasswdCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 385 }

ipRejectCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 386 }

ipRejectLog OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { security 387 }

--  Services status elements

aceNet OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 5026 }

aceManager OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 1149 }

dynamicDnsService OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
```

```
::= { services 5011 }

fullDomainName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { services 5007 }

--  GPS status elements

gpsFix OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 900 }

satelliteCount OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 901 }

latitude OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 902 }

longitude OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 903 }

heading OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 904 }

speed OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 905 }
```

```
engineHours OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { gps 906 }

--  Serial status elements

serialPortMode OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 1043 }

tcpAutoAnswer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 1048 }

udpAutoAnswer OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 1054 }

serialPacketsSent OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 273 }

serialPacketsRecvd OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { serial 274 }

--  About status elements

deviceModel OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
```

```
::= { about 7 }


radioModelType OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 9 }

radioFirmwareVersion OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 8 }

deviceID OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 25 }

macAddress OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 66 }

aleosSWVersion OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 4 }

deviceHwConfiguration OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 5 }

msciVersion OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-only
STATUS current
   DESCRIPTION ""
::= { about 3 }
```

```
-- Read Write values

snmpenable OBJECT-TYPE
SYNTAX INTEGER {
        disabled(0),
        enabled(1)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 10040 }

snmpversion OBJECT-TYPE
SYNTAX INTEGER {
        snmpv2c(2),
        snmpv3(3)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10041 }

snmpport OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10042 }

snmpContact OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  2730 }

snmpName OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  2731 }

snmpLocation OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  2732 }

rocommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
```

```
   DESCRIPTION ""
::= { snmpconfig  10063 }

rouser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10045 }

rosecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
        noauthnopriv(0),
        authnopriv(1),
        authpriv(2)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10046 }

roauthtype OBJECT-TYPE
SYNTAX INTEGER {
        md5(0),
        sha(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10047 }

roauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10048 }

roprivtype OBJECT-TYPE
SYNTAX INTEGER {
        aes(0),
        des(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10049 }

roprivkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10050 }
```

```
rwcommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10064 }

rwuser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10051 }

rwsecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
        noauthnopriv(0),
        authnopriv(1),
        authpriv(2)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10052 }

rwauthtype OBJECT-TYPE
SYNTAX INTEGER {
        md5(0),
        sha(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10053 }

rwauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10054 }


rwprivtype OBJECT-TYPE
SYNTAX INTEGER {
        aes(0),
        des(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10055 }

rwprivkey OBJECT-TYPE
```

```
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10056 }


trapipAddress OBJECT-TYPE
SYNTAX IpAddress
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig 1166 }

trapport OBJECT-TYPE
SYNTAX INTEGER
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10043 }

engineid OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10044 }

trapcommunity OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10065 }

trapuser OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10057 }

trapsecuritylvl OBJECT-TYPE
SYNTAX INTEGER {
        noauthnopriv(0),
        authnopriv(1),
        authpriv(2)}
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10058 }
```

```
trapauthtype OBJECT-TYPE
SYNTAX INTEGER {
        md5(0),
        sha(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10059 }

trapauthkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10060 }


trapprivtype OBJECT-TYPE
SYNTAX INTEGER {
        aes(0),
        des(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10061 }

trapprivkey OBJECT-TYPE
SYNTAX DisplayString
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  10062 }


rebootmodem OBJECT-TYPE
SYNTAX INTEGER {
        nop(0),
        reboot(1) }
MAX-ACCESS read-write
STATUS current
   DESCRIPTION ""
::= { snmpconfig  65001 }



-- Notifications starting at 1000

modemNotifications OBJECT IDENTIFIER ::= { mibversion1  1000 }


value OBJECT-TYPE
   SYNTAX      DisplayString
```

```
    MAX-ACCESS  accessible-for-notify
    STATUS      current
    DESCRIPTION
        "value of MSCIID that triggered this event"
::= { modemNotifications 500 }

digitalInput1 NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Digital Input 1 MSCIID 851"
::= { modemNotifications 1 }


digitalInput2 NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Digital Input 1 MSCIID 852"
::= { modemNotifications 2 }

digitalInput3 NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Digital Input 1 MSCIID 853"
::= { modemNotifications 3 }

digitalInput4 NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Digital Input 1 MSCIID 854"
::= { modemNotifications 4 }

pulseAccumulator1 NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Pulse Accumulator 1 MSCIID 4002"
::= { modemNotifications 5 }


pulseAccumulator2 NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Pulse Accumulator 2 MSCIID 4003"
::= { modemNotifications 6 }

pulseAccumulator3 NOTIFICATION-TYPE
    OBJECTS     { value }
```

```
   STATUS      current
   DESCRIPTION
      "Pulse Accumulator 3 MSCIID 4004"
::= { modemNotifications 7 }

pulseAccumulator4 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Pulse Accumulator 1 MSCIID 4005"
::= { modemNotifications 8 }

analogInput1 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Analog  Input 1 MSCIID 855"
::= { modemNotifications 9 }


analogInput2 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Analog  Input 2 MSCIID 856"
::= { modemNotifications 10 }

analogInput3 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Analog  Input 3 MSCIID 857"
::= { modemNotifications 11 }

analogInput4 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Analog  Input 4 MSCIID 858"
::= { modemNotifications 12 }

scaledAnalogInput1 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
   DESCRIPTION
      "Scaled Analog  Input 1 MSCIID 4041"
::= { modemNotifications 13 }


scaledAnalogInput2 NOTIFICATION-TYPE
   OBJECTS     { value }
   STATUS      current
```

```
    DESCRIPTION
        "Scaled Analog  Input 2 MSCIID 4042"
::= { modemNotifications 14 }

scaledAnalogInput3 NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Scaled Analog  Input 3 MSCIID 4043"
::= { modemNotifications 15 }

scaledAnalogInput4 NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Scaled Analog  Input 4 MSCIID 4044"
::= { modemNotifications 16 }

gpsFixNotification NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "GPS Fix MSCIID 900"
::= { modemNotifications 17 }

vehicleSpeed NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Vehicle Speed MSCIID 905"
::= { modemNotifications 18 }

engineHoursNotification NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Engine Hours MSCIID 906"
::= { modemNotifications 19 }

headingChange NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Heading Change MSCIID 904"
::= { modemNotifications 20 }

rssiNotification NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "RSSI MSCIID 261"
::= { modemNotifications 21 }
```

```
networkStateNotification NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Network State MSCIID 259"
::= { modemNotifications 22 }

networkService NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Network Service 264"
::= { modemNotifications 23 }

networkErrorRate NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Network Error Rate MSCIID 263"
::= { modemNotifications 24 }

periodicReports NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Periodic Reports MSCIID 270"
::= { modemNotifications 25 }

powerInNotification NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Power In  MSCIID 266"
::= { modemNotifications 26 }

boardTemp NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "Board Temperature MSCIID 267"
::= { modemNotifications 27 }

cdmaTemp NOTIFICATION-TYPE
   OBJECTS    { value }
   STATUS     current
   DESCRIPTION
      "CDMA Temperature MSCIID 641"
::= { modemNotifications 28 }


dailyDataUsage NOTIFICATION-TYPE
```

```
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Daily Data Usage MSCIID 25001"
::= { modemNotifications 29 }

monthlyDataUsage NOTIFICATION-TYPE
    OBJECTS     { value }
    STATUS      current
    DESCRIPTION
        "Monthly Data Usage MSCIID 25002"
::= { modemNotifications 30 }

END
```

C: AT Commands

AT Command Set Summary

Note: If you are writing software to parse AT Command responses, Sierra Wireless recommends that you design the software to be independent of the amount of whitespace. Whitespace is defined as ASCII space, tab, carriage return and linefeed characters and may appear in any combination, not necessarily containing all of the above.

Using a terminal connection (Telnet) or SSH protocol, you can send AT commands to configure the device, command it to do something,or query a setting.

- AT commands must always be terminated by a carriage return <CR> (ASCII character 0x0D), i.e., pressing enter on the keyboard. Some may also include a new line or line feed <LF>.
- If E=1 (Echo On), the AT command (including the terminating <carriage return>) is displayed (output) before any responses.
- Two settings affect the format of AT command output: V (Verbose) and Q (Quiet).
- If Q=1 (Quiet On), no result codes are output whatsoever, so there is no response generated by a (non-query) command.
- If Q=0 (Quiet Off), result codes are output. The format of this output is then affected by the Verbose setting.

  If Quiet mode is off, the result code is affected as follows:

  For V=1 (Verbose mode), the textual result code is surrounded by a carriage return and new line. Any AT query response is also surrounded by a carriage return and new line.

  For V=0 (Terse mode), a numeric result code is output with a single trailing carriage return (no new line is output), while any AT query response is followed by a carriage return and new line (there is no preceding output).
- For example, possible output to the AT command “AT” with carriage return (assuming quiet mode is not on) is:

  carriage return — if V=0

  carriage return and new line OK another carriage return and new line — if V=1

Note: AT commands work for the port on which they are executed. For example, if the user types ATE1 and then AT&W using a USB/serial port connection, it sets the USB/serial port to Echo On but not the telnet connection or the RS232 serial port.

If you need to change the port for Telnet (for example, you have the default port blocked on your firewall), the option is on the Services > Telnet/SSH tab. The default Telnet port is 2332. You can also change the Telnet timeout; if the connection is idle, default timeout is 2 minutes. This is the internal Telnet on the device to pass AT commands and not TCP PAD.

AT commands are shown in upper case, but they are not case sensitive.

This appendix organizes the commands into functional groups to allow you to more quickly locate a desired command when you know the operation but not the command. Commands under each topic are listed alphabetically.

Note: Some of the configuration commands listed here are only available as AT commands.

Reference Tables

Result codes are not shown in the command tables unless special conditions apply. Generally the result code OK is returned when the command has been executed. ERROR may be returned if parameters are out of range, and is returned if the command is not recognized or is not permitted in the current state or condition of the AirLink gateway.

Note: Unless otherwise stated, all commands are accessible locally and remotely.

AT command topics in this appendix:

- Standard (Hayes) commands on page 318
- Device Updates on page 284
- Status on page 285
- WAN/Cellular on page 290
- LAN on page 296
- Security on page 304
- Services on page 305
- Serial on page 313
- Standard (Hayes) commands on page 318
- I/O on page 324
- Applications on page 324
- Admin on page 325

Device Updates

Table C-1: Device Update AT Commands

Command	Description
***FWRMUPDATE**	This AT command remotely updates the ALEOS software and if required, the radio module firmware. The ALEOS software file must be on an ftp server, and must have the suffix .bin. If you want to update the radio module firmware as well, that file must also be on the ftp site. The command parameters are: AT*FWRMUPDATE=<FTP Server IP>,<user>,<password>,<ALEOS filename>[,<RM filename>] Where: • <FTP Server IP> is the IP address of the FTP server. • <user> is the user name used to access the FTP server. • <password> is the password used to access the FTP server. • <ALEOS filename> is the name of the ALEOS software file • <RM filename> is the file name for the radio module firmware Example: AT*FWRMUPDATE=192.168.17.111,MyUserName,password,GX_4.4.2.008.bin,MC7700_GCA001_35295.bin Error messages: • Firmware update failed: could not get file from FTP server—Firmware file does not exist; check that the file name was spelled correctly • RM file is required—the update you are attempting requires a radio module update *Note: If the radio module file is missing but required, the update is not completed. If the radio module filename is present, the radio module firmware automatically updates after the ALEOS update is complete.*

Table C-1: Device Update AT Commands (Continued)

Command	Description
***RMUPDATE**	This AT command remotely updates only the radio module firmware. The radio module firmware file must be on an ftp server, and the file name must have the suffix .bin The command parameters are: AT*RMUPDATE=<FTP Server IP>,<user>,<password>,<RM filename> Where: • <FTP Server IP> is the IP address of the FTP server • <user> is the user name used to access the FTP server • <password> is the password used to access the FTP server • <RM filename> is the name of the radio module firmware. Example: AT*RMUPDATE=192.168.17.111,MyUserName,password,MC7700_GCA001_35295.bin

***TPLUPDATE**	This AT command updates the template remotely.
	The template file must be created in ACEmanager, have an .xml file extension, and be accessible on an FTP server.
	The command parameters are:
	AT*TPLUPDATE=<FTP Server IP>,<user>,<password>,<filename>
	where:
	• <FTP Server IP> is the IP address of the FTP server
	• <user> is the user name used to access the FTP server
	• <password> is the password used to access the FTP server
	• <filename> is the name of the template file on the FTP server that you want to apply to the AirLink gateway. The template file must be stored on the FTP User_Name home, not in a sub-folder.
	Example:
	AT*TPLUPDATE=192.168.17.111,MyUserName,MyPassword,NewTemplate.xml
	When the template is successfully applied, the message displayed is:
	`Template applied successfully`
	`OK`
	Note: Configure the FTP server:
	• *As passive mode (not active mode)*
	• *To listen to port 21*

Status

Command	Description
***BAND?**	HSPA and LTE fallback to HSPA only. Query the current radio module band.
***CELLINFO?**	Query cellular connection information.
***CELLINFO2?**	Query in depth cell information.

Command	Description
+CIMI?	HSPA and LTE only. Query the IMSI.
***DEVICEID?**	When the device is configured to use the device ID, this command displays the 64-bit device ID created from the ESN/IMEI or phone, preceded by the hex delimiter (0x). For example: at*deviceid? 0x010112DE140B5A32
***DNS1?** ***DNS2?**	Query the primary DNS (*DNS1) and secondary (*DNS2) IP addresses. AT*DNS1? to query DNS1 AT*DNS2? to query DNS2
+ECIO?	Query the signal quality.
***ETHMAC?**	Query the MAC address of the Ethernet port • AT*ETHMAC? or AT*ETHMAC?1— Returns the MAC address of the main Ethernet port
***ETHSTATE?**	Query the connection state (speed and duplex) of the Ethernet port. • AT*ETHSTATE? or AT*ETHSTATE?1— Returns the speed and duplex state of the main Ethernet port (e.g. 100Mb/s Full Duplex)
***GLOBALID?**	Query the global ID used by AVMS to identify the device.
***HOSTCOMMLVL?**	Query the serial host signal level. Response example: DCD:LOW; DTR:LOW; DSR:HIGH; CTS:HIGH; RTS:LOW
+HWTEMP?	Query the internal temperature of the radio module (in degrees Celsius).
I[n]	Query device information. • n omitted—device model • n=0—device model • n=1—ALEOS software version, hardware revision, boot version • n=2—Radio module firmware version • n=3—Radio module's unique ID (ESN, IMIEI, or EID)
+ICCID?	HSPA and LTE only. Query the SIM ID.
***LTERSRQ?**	LTE only Query the LTE signal quality (in dB). For more information, see LTE Signal Quality (RSRQ) on page 33.
***LTERSRP?**	LTE only Query the LTE signal strength (in dBm). For more information, see LTE Signal Strength (RSRP) on page 33.
***NETCHAN?**	Query the current cellular network channel.

Command	Description
NETIP?	Query the current WAN IP address of the device reported by the internal module (generally obtained from your Mobile Network Operator). If you have an Internet-routable IP address, you can use this address to contact devices from the Internet. If your device is on a private cellular network, you can use this address to contact the device from another host on the same WAN network. If required, use AT**NETALLOWZEROIP to allow displaying an IP address ending in a zero. *Note: If there is no current network IP address, 0.0.0.0 is returned.*
***NETOP?**	Query the Mobile Network Operator of the active connection. If you are roaming, the roaming operator is returned, if the home operator allows this.
***NETPHONE?**	Query the device's cellular phone number, if applicable or obtainable.
***NETRSSI?**	Query the current RSSI (Receive Signal Strength Indicator) for non-LTE cellular connections, as a negative dBm value.
***NETSERV?**	Query the current connection type (e.g., LTE, HSPA+, EV-DO Rev A, etc.).
***NETSERVICE_RAW?**	Query the numeric value for the network service type. • 8—2G (1x, EDGE, GPRS) • 10—2G roaming • 16—3G (EV-DO Rev. A, HSPA, HSPA+, UMTS) • 18—3G roaming • 64—4G

Command	Description
***NETSTATE?**	Query the network state of the current WAN connection. AT*NETSTATE? returns: • Connecting To Network—The device is in the process of trying to connect to the cellular network. • Network Authentication Fail—Authentication to the cellular network has failed. Verify settings to activate the device. • Data Connection Failed—The device failed to connect, and it is now waiting a set time interval before it attempts to reconnect. Verify settings to activate the device. • Network Negotiation Fail—Network connection negotiation failed. This is usually temporary and often clears up during a subsequent attempt. • Network Ready—The device is connected to the 1x cellular network and ready to send data. • Network Dormant—The device is connected to the 1x cellular network, but the link is dormant. It will be woken up when data is sent or received. • No Service—There is no cellular network detected. • Hardware Reset—The internal module is being reset. This is a temporary state. • No SIM or Unexpected SIM status—No SIM, SIM installed incorrectly, or another SIM error. • Awaiting Provisioning—An EV-DO device without an account and hasn't had an account or the provisioning has been erased from the radio. • Provisioning... —An EV-DO device in the process of writing the account data to the radio. • SIM Locked, but bad SIM PIN. • SIM PIN incorrect 3 attempts left. • SIM PIN incorrect 2 attempts left. • SIM PIN incorrect 1 attempts left. • SIM PIN incorrect 0 attempts left. • SIM Blocked, Bad unlock code. • SIM Blocked, unblock code incorrect.

Command	Description
***NETSTATE_RAW?**	Query numeric value of the network state of the current WAN connection: • 1—Connecting To Network—The device is in the process of trying to connect to the cellular network. • 4—Network Access Denied—Connection rejected. • 5—Network Ready—WAN is using cellular and is online. • 7—No Service—The WAN link is down or unavailable • 9—No SIM or Unexpected SIM status—No SIM, SIM installed incorrectly, or another SIM error. • 11—Awaiting Provisioning—An EV-DO device without an account and hasn't had an account or the provisioning has been erased from the radio. • 12—Data Connection Failed - Waiting to Retry—The device failed to connect, and it is waiting a set time interval before it attempts to reconnect. Or • 12—Provisioning... —An EV-DO device in the process of writing the account data to the radio. • 13—SIM Locked, but bad SIM PIN. • 14—SIM PIN incorrect 3 attempts left. • 15—SIM PIN incorrect 2 attempts left. • 16—SIM PIN incorrect 1 attempts left. • 17—SIM PIN incorrect 0 attempts left. • 18—SIM Blocked, Bad unlock code. • 19—SIM Blocked, unblock code incorrect.
+PRL?	CDMA and LTE fallback to EV-DO only Query CDMA Preferred Roaming List (PRL) version.
***PRLSTATUS?**	CDMA only Query the status of the most recent PRL update • n=0—None (No update) • n=1—In progress • n=2—Update successful The return of any other value indicates that the update failed.
***USBNETSTATE?**	Query the status of the USB connection. AT*USBNETSTATE? returns: • None—There are no USB connections to the AirLink gateway. • 8 MB/s Half Duplex—There is a USB connection to the device.
***WANUPTIME?**	Query the time in minutes from which the cellular IP is obtained from the mobile network. AT*WANUPTIME?

WAN/Cellular

A reboot is required before the WAN/Cellular AT Commands described in the following table take effect.

Table C-2: WAN/Cellular AT Commands

Command	Description
***AUTOPRL**	CDMA only. Query or set automatic Preferred Roaming List updates AT*PRL? to query AT*PRL=n to set • n=0—Disable • n=1—Enable *Note: To query the current PRL, use +PRL?.*
***AUTOPRLFREQ**	CDMA only. Query or set how often the PRL automatically updates. AT*AUTOPRLFREQ? to query AT*AUTOPRLFREQ=n to set • n=interval to check for updates (in days)
!BAND	HSPA and LTE fallback to HSPA only. Query or set the RF band range or technology. AT!BAND? to query a value sent since the device was last rebooted. AT!BAND=hh to set at the next reboot. • hh=00—All bands • hh=03—GSM 900/1800 • hh=05—GSM All • hh=08—WCDMA All • hh=10—WCDMA 900/2100 *Note: For some Mobile Network Operator SIM Cards, you may need to set the radio band before installing the SIM card.*

Table C-2: WAN/Cellular AT Commands (Continued)

Command	Description
+CGDCONT	HSPA only Query or set the PDP context, APN, and other information required to establish a connection to o an HSPA network. You only need to configure this once. The parameters are saved and used each time a connection is made to the HSPA network. AT+CGDCONT? to query AT+CGDCONT = PID,PDP_TYPE,APN [,IPADDR] to set PID= PDP context identifier PDP_TYPE = numeric parameter that specifies a PDP context definition APN = Access Point Name IPADDR = IP address Examples: AT+CGDCONT=1,IP,proxy AT+CGDCONT=1,IP,internet *Note: When using the APN-related optons in ACEmanager, you generally do not need to configure +CGDCONT.*
***CLIENT_PPP_AUTH**	Query or set the Force Network Authentication mode. AT*CLIENT_PPP_AUTH? to query AT*CLIENT_PPP_AUTH=n to set • n=0—None • n=1—PAP • n=2—CHAP
+COPS	HSPA only Query or set the network operator and the connection mode. AT+COPS? to query AT+COPS=MODE[,FORMAT[,OPER]] to set MODE • MODE=0—Automatic (default) • MODE=1—Manual • MODE=4—Manual/Automatic; if manual failed, it defaults to automatic FORMAT • FORMAT=0—Alphanumeric (“Name”) • FORMAT=2—Numeric OPER • OPER=the operator numeric code Example, AT+COPS=1,2,302610 Manual mode, numeric format, operator code 302610 *Note: On some mobile networks, explicit use of +COPS allows you to select the roaming Mobile Network Operator to use.*

Table C-2: WAN/Cellular AT Commands (Continued)

Command	Description
***EVDODATASERV**	CMDA and LTE fallback to EV-DO only. Query or set the allowable network type. AT*EVDODATASERV? to query AT*EVDODATASERV=n to set • n=0—EV-DO Preferred—can "fall back" on CDMA/1x (only available on EV-DO devices) • n=0—LTE Preferred—can "fall back" on CDMA/EV-DO (only available on LTE devices) • n=1—EV-DO Only—Fallback disabled (only available on 1x/EV-DO devices) • n=2—1x Only—EV-DO disabled (only available on 1x/EV-DO devices) • n=3—CDMA Only—LTE disabled (only available on LTE devices) • n=4—LTE Only—Fallback disabled (only available on LTE devices) *Note: If you choose one of the options where fall back is disabled and the selected network type is not available, the device will not be able to connect to the mobile network. For example, if you select LTE Only and you are in an area where there is no LTE network available, the device will not be able to connect to a mobile network until you change this setting or move to an area with LTE coverage.*
***EVDODIVERSITY**	CDMA only. For HSPA device, see *RXDIVERSITY on page 295. Query or set EV-DO Diversity, which allows two antennas to provide more consistent connection. AT*EVDODIVERSITY? to query AT*EVDODIVERSITY=n to set • n=0—Disabled • n=1—Enabled *Note: If you are not using a diversity antenna, *EVDODIVERSITY should be disabled.*
***EVDOROAMPREF**	CDMA and LTE fallback to EV-DO only Query or set the network roaming preference AT*EVDOROAMPREF? to query AT*EVDOROAMPREF=n to set • n=0—Automatic • n=1—Home only
***HANGUPTORESET**	HSPA only. Query or set forcing the radio module to reset when the device disconnects. AT*HANGUPTORESET? to query AT*HANGUPTORESET=n to set • n=0—Disable • n=1—Enable

Table C-2: WAN/Cellular AT Commands (Continued)

Command	Description
***IPPING**	Query or set the interval between keepalive pings (in minutes) if no valid packets have been received by the IP address or FQDN specified in *IPPINGADDR. AT*IPPING? to query the Keepalive PING time interval AT*IPPING=n to set the Keepalive PING time interval • n=0—Disable pinging (default) • n=15–255 minutes *Note: 15 minutes is the minimum interval for Keep Alive. If you set *IPPING for a value between 0 and 15, the idle interval for pings will be 15 minutes.*
***IPPINGADDR**	Query or set the Keepalive PING IP address or FQDN for the device to ping when Keepalive Ping Time (*IPPING) is set. AT*IPPINGADDR? to query AT*IPPINGADDR=[d.d.d.d] or [n] • d.d.d.d=IP address • n=domain name *Note: AT*IPPING must to be set to a value other than 0 to enable pinging.*
***IPPINGFORCE**	Query or set the Force Keepalive Ping setting. When this feature is enabled, the Keepalive ping is sent even if IP traffic has occurred during the configured interval. AT*IPPINGFORCE? to query AT*IPPINGFORCE=n to set • n=0—Disable • n=1—Enable *Note: To enable this command, *IPPING must be enabled and *IPPINGADDR configured.*
***NETALLOWZEROIP**	Query or set allowing the device to get an IP address from the mobile network that has the last octet as 0 (zero). AT*NETALLOWZEROIP? to query AT*NETALLOWZEROIP=n to set • n=0—Do not allow • n=1—Allow Allows the device to use a WAN IP address that ends in zero (e.g. 192.168.1.0).
***NETAPN**	HSPA and LTE fallback to HSPA only Query or set the user entered APN. AT*NETAPN? to query AT*NETAPN=APN to set (up to 80 characters) *Note: When you set this command, the APN type is automatically set to User Entry so that the APN you enter with this AT command is used on reboot.*

Table C-2: WAN/Cellular AT Commands (Continued)

Command	Description
***NETPW**	Set the mobile network account password, if required. AT*NETPW=PW to set (up to 30 characters) *Note: AT*NETPW? returns a dotted display for privacy.*
***NETUID**	Query or set the mobile network account user ID, if required. AT*NETUID? to query AT*NETUID=USER ID (up to 64 bytes)
***NWDOGTIME**	Query or set the interval that the network connection watchdog waits for a cellular or W-Fi WAN connection. If no connection is established within this interval, the device resets. AT*NWDOGTIME? to query AT*NWDOGTIME=n to set Accepted values: • n=0—Disable • n=5—5 Minutes • n=10—10 Minutes • n=15—15 Minutes • n=30—30 Minutes • n=45—45 Minutes • n=60—1 Hour • n=120—2 Hours (default) • n=180—3 Hours • n=240—4 Hours *Note: This AT Command replaces AT*NETWDOG.*
PING	Sends 5 PING to a single address. Returns OK if there is a response: ERROR if there is no response. ATPING[ip address or FQDN] *Note: Do not use an equal sign (=) when issuing the command.* Example: ATPINGsierrawireless.com
$QCMIP	CDMA and LTE fallback to EV-DO only Query or set use of Mobile IP (MIP) preferences. $QCMIP? to query $QCMIP=n to set • n=0—Disabled, Simple IP (SIP) only • n=1—Mobile IP preferred • n=2—Mobile IP only

Table C-2: WAN/Cellular AT Commands (Continued)

Command	Description

***RADIO_CONNECT**	This AT Command applies only to International devices on the Vodafone network.
	Query or set the wireless connection setting.
	AT*RADIO_CONNECT? to query
	AT*RADIO_CONNECT=n to set
	• n=0—Disables data traffic. The only way to change this mode is to issue a radio_connect=1 or radio_connect=2 AT command.
	• n=1—Enables Always on connection.
	• n=2—Disables Always on connection. The device listens for outgoing traffic and establishes a mobile network data connection for a specified time:
	  • When there is outgoing traffic
	  or
	  • When it receives a Wakeup SMS, provided Wakeup SMS is configured.
	  (Use *TRAFWUPTOUT on page 296 to set the timeout period.)
	Note: This command is not persistent over device resets.
	Note: You can only send this command locally over a serial, serial USB, or local telnet/SSH connection.

***RADIO_CONNECT_STARTUP**	This AT Command applies only to International devices on the Vodafone network. You can query this command remotely or locally, but it can only be set locally. This command is the same as *RADIO_CONNECT, except • The change does not take effect until the next reboot. • The setting is persistent over subsequent reboots.
***RXDIVERSITY**	HSPA only. For CDMA devices, see *EVDODIVERSITY on page 292. Query or set the RX Diversity setting. Rx Diversity allows you to use two antennas for a more consistent connection. If you are not using a diversity antenna, Rx Diversity should be disabled. AT*RXDIVERSITY? to query AT*RXDIVERSITY=n to set • n=0—Disable • n=1—Enable *Note: This AT Command is not available for all AirLink gateways.*
***SIMPIN**	HSPA and LTE fallback to HSPA only Query or enter the SIM pin. AT*SIMPIN? to query AT*SIMPIN=n to enter the SIM pin

Table C-2: WAN/Cellular AT Commands (Continued)

Command	Description
***SIMPINENABLE**	HSPA and LTE fallback to HSPA only Query or set the SIM pin. AT*SIMPINENABLE? to query AT*SIMPINENABLE=n to set • n=0—Don't change • n=1—Enable (SIM pin required on startup) • n=2—Disable
***TRAFWUPTOUT**	This AT Command applies only to International devices on the Vodafone network. Query or set the timeout period after which, if there is no outgoing WAN traffic, the connection is terminated. The timeout period only takes effect if *RADIO_CONNECT or *RADIO_CONNECT_STARTUP is set to 1, or Always on connection is disabled in ACEmanager. (See Always on connection on page 57.) AT*TRAFWUPTOUT? to query AT*TRAFWUPTOUT=n to set • n=2–65535 minutes (default is 2) *Note: This timer is reset to zero each time a WAN packet goes out.*

LAN

Note: A reboot is required before these commands take effect.

Table C-3: LAN AT Commands

Command	Description
***DHCPHOSTEND**	Query or set the ending IP address for the Ethernet DHCP pool AT*DHCPHOSTEND? to query AT*DHCPHOSTEND=d.d.d.d to set • d.d.d.d=last IP address in Ethernet DHCP pool
***DHCPNETMASK**	Query or set the Ethernet DHCP subnet mask AT*DHCPNETMASK? to query AT*DHCPNETMASK=d.d.d.d to set • d.d.d.d=Ethernet DHCP subnet mask
***DHCPSERVER**	Query or set the Ethernet DHCP server. AT*DHCPSERVER? to query AT*DHCPSERVER=n to set the DHCP server mode • n=0—Disable • n=1—Server • n=2—Auto For a description of the settings, see DHCP Mode on page 88.

Table C-3: LAN AT Commands (Continued)

Command	Description
***DNS1?** ***DNS2?**	Query the primary DNS (*DNS1) and secondary (*DNS2) IP addresses. AT*DNS1? to query DNS1 AT*DNS2? to query DNS2
***DNSUSER**	Query or set the first alternate server for DNS override. (Applies only to primary DNS.) AT*DNSUSER? to query AT*DNSUSER=d.d.d.d • d.d.d.d=IP address of domain server
***HOSTAUTH**	Query or set the Host Authentication mode for PPPoE only. (It does not set host authentication for PPP/DUN.) AT*HOSTAUTH? to query AT*HOSTAUTH=n to set • n=0—None/Disables authentication for PPPoE (default). • n=1— Authentication through PAP • n=2—Authentication through PAP & CHAP
***HOSTPEERIP**	Query or set the IP address of the device's Ethernet port. By default this is 192.168.13.31. *Note: Any connected LAN host can access this IP addresses, whether using a private or public IP address. This IP address must be in the same subnet as the Ethernet DHCP pool.* AT*HOSTPEERIP? to query AT*HOSTPEERIP=d.d.d.d to set • d.d.d.d=local or peer IP address of the device
***HOSTPRIVIP**	Query or set the starting IP for the Ethernet DHCP pool. AT*HOSTPRIVIP? to query AT*HOSTPRIVIP=d.d.d.d to set • d.d.d.d=IP Address
***HOSTPRIVMODE**	Query or set the host communication mode used for tethered IP connections. AT*HOSTPRIVMODE? to query AT*HOSTPRIMODE=n to set which user interface uses the Public IP address • n=0—Ethernet Uses Public IP • n=1—All Hosts Use Private IPs • n=2—USB Uses Public IP • n=3—DUN Uses Public IP • n=4—First Host gets Public IP
***HOSTPW**	Query or set the host password for PPPoE only. (It does not set the password for PPP/DUN.) AT*HOSTPW? to query AT*HOSTPW=PASSWORD to set *Note: PASSWORD cannot be "password".*

Table C-3: LAN AT Commands (Continued)

Command	Description
***HOSTUID**	Query or set the Host user ID for PPPoE only. (It does not set the user ID for PPP/DUN.) AT*HOSTUID? to query AT*HOSTUID=USER ID to set (up to 64 bytes) *Note: USER ID cannot be "user".*
***USBDEVICE**	Query or set the startup mode for the USB port. AT*USBDEVICE? to query AT*USBDEVICE=n to set • n=0 — USB Serial • n=1 — USBNET • n=2 — Disabled

VPN

Table C-4: VPN Commands

Command	Description
***IPSEC1_AUTH** ***IPSEC2_AUTH** ***IPSEC3_AUTH** ***IPSEC4_AUTH** ***IPSEC5_AUTH**	Query or set the authentication type for # VPN. AT*IPSEC[VPN number]_AUTH? to query AT*IPSEC[VPN number]_AUTH=n to set • n=0 — None • n=1 — MD5 • n=2 — SHA1 (default) • n=3 — SHA 256 *Note: MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests.*
***IPSEC1_DH** ***IPSEC2_DH** ***IPSEC3_DH** ***IPSEC4_DH** ***IPSEC5_DH**	Query or set how the AirLink gateway VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during the phase 1 authentication. The AirLink gateway supports three prime key lengths, including Group 1 (768 bits), Group 2 (1,024 bits), and Group 5 (1,536 bits). AT*IPSEC[VPN number]_DH? to query AT*IPSEC[VPN number]_DH=n to set • n=0 — None • n=1 — DH1 • n=2 — DH2 (default) • n=5 — DH5
***IPSEC1_ENCRYPT** ***IPSEC2_ENCRYPT** ***IPSEC3_ENCRYPT** ***IPSEC4_ENCRYPT** ***IPSEC5_ENCRYPT**	Query or set the type/length of encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets for # VPN. AT*IPSEC[VPN number]_ENCRYPT? to query AT*IPSEC[VPN number]_ENCRYPT=n to set • n=0 — None • n=1 — DES • n=2 — 3DES • n=3 — AES-128 (default) • n=7 — AES-256 *Note: 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption.*
***IPSEC1_GATEWAY** ***IPSEC2_GATEWAY** ***IPSEC3_GATEWAY** ***IPSEC4_GATEWAY** ***IPSEC5_GATEWAY**	Query or set the IP address of the server that # VPN client connects to. AT*IPSEC[VPN number]_GATEWAY? to query AT*IPSEC[VPN number]_GATEWAY=[IP address] to set

Table C-4: VPN Commands (Continued)

Command	Description
***IPSEC1_IKE_AUTH** ***IPSEC2_IKE_AUTH** ***IPSEC3_IKE_AUTH** ***IPSEC4_IKE_AUTH** ***IPSEC5_IKE_AUTH**	Query or set the IKE authentication type for # VPN. AT*IPSEC[VPN number]_IKE_AUTH? to query AT*IPSEC[VPN number]_IKE_AUTH=n to set • n=1 — MD5 • n=2 — SHA1 • n=3 — SHA 256 *Note: MD5 is an algorithm that produces a 128-bit digest for authentication. SHA is a more secure algorithm that produces both 160-bit (SHA1) and 256-bit (SHA256) digests.*
***IPSEC1_IKE_DH** ***IPSEC2_IKE_DH** ***IPSEC3_IKE_DH** ***IPSEC4_IKE_DH** ***IPSEC5_IKE_DH**	Query or set how the AirLink gateway VPN creates an SA with the VPN server. The DH (Diffie-Hellman) key exchange protocol establishes pre-shared keys during the phase 1 authentication. The AirLink gateway supports three prime key lengths, including Group 1 (768 bits), Group 2 (1,024 bits), and Group 5 (1,536 bits). AT*IPSEC[VPN number]_IKE_DH? to query AT*IPSEC[VPN number]_IKE_DH=n to set • n=1 — DH1 • n=2 — DH2 (default) • n=5 — DH5
***IPSEC1_IKE_ENCRYPT** ***IPSEC2_IKE_ENCRYPT** ***IPSEC3_IKE_ENCRYPT** ***IPSEC4_IKE_ENCRYPT** ***IPSEC5_IKE_ENCRYPT**	Query or set the type/length of IKE encryption key used to encrypt/decrypt ESP (Encapsulating Security Payload) packets for # VPN. AT*IPSEC[VPN number]_IKE_ENCRYPT? to query AT*IPSEC[VPN number]_IKE_ENCRYPT=n to set • n=1 — DES • n=5 — 3DES • n=7 — AES-128 (default) • n=9 — AES-256 *Note: 3DES supports 168-bit encryption. AES (Advanced Encryption Standard) supports both 128-bit and 256-bit encryption.*
***IPSEC1_IKE_LIFETIME** ***IPSEC2_IKE_LIFETIME** ***IPSEC3_IKE_LIFETIME** ***IPSEC4_IKE_LIFETIME** ***IPSEC5_IKE_LIFETIME**	Query or set how long the # VPN tunnel is active (in seconds). AT*IPSEC[VPN number]_IKE_LIFETIME? to query AT*IPSEC[VPN number]_IKE_LIFETIME=n to set • n= 180–86400 • Default is 7200.
***IPSEC1_LIFETIME** ***IPSEC2_LIFETIME** ***IPSEC3_LIFETIME** ***IPSEC4_LIFETIME** ***IPSEC5_LIFETIME**	Query or set how long the # VPN tunnel is active (in seconds). AT*IPSEC[VPN number]_LIFETIME? to query AT*IPSEC[VPN number]_LIFETIME=n to set • n= 180–86400 • Default is 7200.

Table C-4: VPN Commands (Continued)

Command	Description
***IPSEC1_LOCAL_ADDR** ***IPSEC2_LOCAL_ADDR** ***IPSEC3_LOCAL_ADDR** ***IPSEC4_LOCAL_ADDR** ***IPSEC5_LOCAL_ADDR**	Query or set the device subnet address for # VPN. AT*IPSEC[VPN number]_LOCAL_ADDR? returns the device subnet address AT*IPSEC[VPN number]_LOCAL_ADDR=[subnet address] to set
***IPSEC1_LOCAL_ADDR_MASK** ***IPSEC2_LOCAL_ADDR_MASK** ***IPSEC3_LOCAL_ADDR_MASK** ***IPSEC4_LOCAL_ADDR_MASK** ***IPSEC5_LOCAL_ADDR_MASK**	Query or set the device subnet mask information (24-bit netmask) AT*IPSEC[VPN number]_LOCAL_ADDR_MASK? to query AT*IPSEC[VPN number]_LOCAL_ADDR_MASK =[subnet mask] to set Default is 255.255.255.0
***IPSEC1_LOCAL_ADDR_TYPE** ***IPSEC2_LOCAL_ADDR_TYPE** ***IPSEC3_LOCAL_ADDR_TYPE** ***IPSEC4_LOCAL_ADDR_TYPE** ***IPSEC5_LOCAL_ADDR_TYPE**	Query or set the network address type for # VPN. AT*IPSEC[VPN number]_LOCAL_ADDR_TYPE? to query AT*IPSEC[VPN number]_LOCAL_ADDR_TYPE=n to set • n=1 — Use the Host Subnet • n=5 — Single Address • n=17 — Subnet Address (default)
***IPSEC1_LOCAL_ID** ***IPSEC2_LOCAL_ID** ***IPSEC3_LOCAL_ID** ***IPSEC4_LOCAL_ID** ***IPSEC5_LOCAL_ID**	Query or set the local (My Identity) ID for the # VPN. • If IP is selected as the local (My Identity) type, AT*IPSEC[VPN number]_LOCAL _ID? returns the WAN IP address assigned by the Mobile Network Operator • If FQDN or User FQDN is selected as the local (My Identity) type, AT*IPSEC[VPN number]_LOCAL_ID? returns the FQDN (for example me@mycompany.com) To set the local ID: AT*IPSEC[VPN number]_LOCAL _ID=[IP address] or [FQDN], depending on the setting for Local ID (My Identity) type.
***IPSEC1_LOCAL_ID_TYPE** ***IPSEC2_LOCAL_ID_TYPE** ***IPSEC3_LOCAL_ID_TYPE** ***IPSEC4_LOCAL_ID_TYPE** ***IPSEC5_LOCAL_ID_TYPE**	Query or set the local (My Identity) ID type for the # VPN. AT*IPSEC[VPN number]_LOCAL_ID_TYPE? to query AT*IPSEC[VPN number]_LOCAL_ID_TYPE=n to set • n=1 — IP • n=2 — FQDN • n=3 — User FQDN *Note:* • *IP (default) allows you to use an IP address* • *FQDN allows you to use a fully qualified domain name (FQDN) e. g., modemname.domainname.com* • *User FQDN allows you to use a user FQDN whose values should include a username (e.g. user@domain.com)*

Table C-4: VPN Commands (Continued)

Command	Description
***IPSEC1_NEG_MODE** ***IPSEC2_NEG_MODE** ***IPSEC3_NEG_MODE** ***IPSEC4_NEG_MODE** ***IPSEC5_NEG_MODE**	Query or set the negotiation mode for # VPN. AT*IPSEC[VPN number]_NEG_MODE? returns AT*IPSEC[VPN number]_NEG_MODE=n to set • n=1 — Main • n=2 — Aggressive *Note: Aggressive mode offers increased performance at the expense of security.*
***IPSEC1_PFS** ***IPSEC2_PFS** ***IPSEC3_PFS** ***IPSEC4_PFS** ***IPSEC5_PFS**	Query or set the Perfect Forward Secrecy (PFS) setting for # VPN. PFS provides additional security through a DH shared secret value. When this feature is enabled, one key cannot be derived from another. This ensures previous and subsequent encryption keys are secure even if one key is compromised. AT*IPSEC[VPN number]_PFS? to query PFS AT*IPSEC[VPN number]_PFS=n to set PFS • n=0 — Yes (default) • n=1 — No
***IPSEC1_REMOTE_ADDR** ***IPSEC2_REMOTE_ADDR** ***IPSEC3_REMOTE_ADDR** ***IPSEC4_REMOTE_ADDR** ***IPSEC5_REMOTE_ADDR**	Query or set the IP address of the device behind the gateway for # VPN. AT*IPSEC[VPN number]_REMOTE_ADDR? to query AT*IPSEC[VPN number]_REMOTE_ADDR=[IP address] to set
***IPSEC1_REMOTE_ADDR_MASK** ***IPSEC2_REMOTE_ADDR_MASK** ***IPSEC3_REMOTE_ADDR_MASK** ***IPSEC4_REMOTE_ADDR_MASK** ***IPSEC5_REMOTE_ADDR_MASK**	Query or set the remote subnet mask information (24-bit netmask). AT*IPSEC[VPN number]_REMOTE_ADDR_MASK? to query AT*IPSEC[VPN number]_REMOTE_ADDR_MASK =[subnet mask] to set Default is 255.255.255.0
***IPSEC1_REMOTE_ADDR_TYPE** ***IPSEC2_REMOTE_ADDR_TYPE** ***IPSEC3_REMOTE_ADDR_TYPE** ***IPSEC4_REMOTE_ADDR_TYPE** ***IPSEC5_REMOTE_ADDR_TYPE**	Query or set network information of the IPsec server behind the IPsec gateway for # VPN. AT*IPSEC[VPN number]_REMOTE_ADDR_TYPE? to query AT*IPSEC[VPN number]_REMOTE_ADDR_TYPE=n to set • n=5 — Single Address • n=17 — Subnet Address (default)
***IPSEC1_REMOTE_ID** ***IPSEC2_REMOTE_ID** ***IPSEC3_REMOTE_ID** ***IPSEC4_REMOTE_ID** ***IPSEC5_REMOTE_ID**	Query or set the remote (Peer Identity) ID for the # VPN. • If IP is selected as the remote (Peer Identity) type, AT*IPSEC[VPN number]_REMOTE_ID? returns the WAN IP address assigned by the Mobile Network Operator • If FQDN or User FQDN is selected as the remote (Peer Identity) type, AT*IPSEC[VPN number]_REMOTE_ID? returns the FQDN (for example me@mycompany.com) To set the remote ID: AT*IPSEC[VPN number]_REMOTE _ID=[IP address] or [FQDN], depending on the setting for remote ID (Peer Identity) type.

Table C-4: VPN Commands (Continued)

Command	Description
***IPSEC1_REMOTE_ID_TYPE** ***IPSEC2_REMOTE_ID_TYPE** ***IPSEC3_REMOTE_ID_TYPE** ***IPSEC4_REMOTE_ID_TYPE** ***IPSEC5_REMOTE_ID_TYPE**	Query or set the remote (Peer Identity) ID type for the # VPN. AT*IPSEC[VPN number]_REMOTE_ID_TYPE? to query AT*IPSEC[VPN number]_REMOTE_ID_TYPE=n to set • n=1 — IP • n=2 — FQDN • n=3 — User FQDN *Note:* • *FQDN allows you to use a fully qualified domain name (FQDN) e. g., modemname.domainname.com* • *User FQDN allows you to use a user FQDN whose values should include a username (e.g. user@domain.com)*
***IPSEC1_SHARED_KEY1** ***IPSEC2_SHARED_KEY1** ***IPSEC3_SHARED_KEY1** ***IPSEC4_SHARED_KEY1** ***IPSEC5_SHARED_KEY1**	Query the pre-shared Key (PSK) used to initiate the # VPN tunnel. AT*IPSEC[n]_SHARED_KEY1? [n]=server number
***IPSEC1_STATUS?** ***IPSEC2_STATUS?** ***IPSEC3_STATUS?** ***IPSEC4_STATUS?** ***IPSEC5_STATUS?**	Query the VPN # connection status. AT*IPSEC[VPN number]_STATUS? to query • Disabled • Not Connected • Connected *Note: Use this when troubleshooting a VPN # connection.*
***IPSEC1_TUNNEL_TYPE** ***IPSEC2_TUNNEL_TYPE** ***IPSEC3_TUNNEL_TYPE** ***IPSEC4_TUNNEL_TYPE** ***IPSEC5_TUNNEL_TYPE**	Query or set the VPN # tunnel type. AT*IPSEC[VPN number]_TUNNEL_TYPE? to query AT*IPSEC[VPN number]_TUNNEL_TYPE=n to set • n=0 — Disable the tunnel (default) • n=1 — IPsec Tunnel • n=2 — GRE Tunnel • n=3 — SSL Tunnel *Note: For a successful configuration, all settings for the VPN tunnel must be identical between the AirLink gateway VPN and the enterprise VPN server.*

Security

Table C-5: Security AT Commands

Command	Description
F0 (F1, F2, ... F9)	Query or set the Inbound Trusted IP List. ATF? to query the list ATF[n]=d.d.d.d to set • n=0–9 Trusted IP list index number • d.d.d.d = IP Address Using 255 in the IP address will allow any number Example: 166.129.2.255 allows access by all IPs in the range 166.129.2.0–166.129.2.255. Example: atf? 0=192.32.32.21 1=192.32.32.22 2=192.32.32.23 3=0.0.0.0 4=0.0.0.0 5=0.0.0.0 6=0.0.0.0 7=0.0.0.0 8=0.0.0.0 9=0.0.0.0 OK If the index number does not have an IP address associated with it, the query returns 0.0.0.0 for that index number. *Note: You can only query or configure the first nine Inbound Trusted IP addresses with this AT Command. You cannot query or configure Trusted range entries with this AT Command.*
FM	Query or set the Inbound Trusted IP mode (Friends List) — Only allow specified IPs to access the device. ATFM? to query the setting ATFM=n to set • n=0 — Disable Trusted IP mode • n=1 — Enable Trusted IP mode — Only packets from IP addresses in the Trusted IP list are allowed. Packets from other IP addresses are ignored.

Services

Table C-6: Services AT Commands

Command	Description
AirVantage Management System	
***AVMS_ENABLE**	Query or set the AVMS activation status. AT*AVMS_ENABLE? to query AT*AVMS_ENABLE=n to set • n=0—Disable device initiated AVMS management • n=1—Enable device initiated AVMS management
***AVMS_INTERVAL**	Query or set the AVMS communication (heartbeat) interval in minutes. AT*AVMS_INTERVAL? to query AT*AVMS_INTERVAL= n to set • n= INTERVAL (in minutes)
***AVMS_NAME**	Assigns or queries the name to the AirLink gateway as it appears in AVMS. AT*AVMS_NAME? to query AT*AVMS_NAME= n to set • n= AVMS NAME
***AVMS_SERVER**	Query or set the AVMS server IP address or FQDN. AT*AVMS_SERVER? to query AT*AVMS_SERVER=n to set • n=IP Address or FQDN of AVMS server
***AVMS_STATUS?**	Query the AVMS connection status
***AVMS_AUTOSYNC**	Query or set AVMS autosynchronization of configuration parameters. AT*AVMS_AUTOSYNC? to query AT**AVMS_AUTOSYNC=n to set • n=0—Disable AVMS autosynchronization • n=1—Enable AVMS autosynchronization
***AVMS_VERIFYPEER**	Query or set peer certificate verification during SSL handshake. AT*AVMS_VERIFYPEER? to query AT*AVMS_VERIFYPEER=n to set • n=0—Disable peer certificate verification during SSL handshake • n=1—Enable peer certificate verification during SSL handshake
Dynamic DNS	

Table C-6: Services AT Commands (Continued)

Command	Description
***DOMAIN**	Query or set the domain name used for the IP Manager Dynamic DNS configuration. AT*DOMAIN? to query AT*DOMAIN=DOMAIN to set (up to 20 characters) Example: AT*DOMAIN=eairlink.com **Tip:** *Only letters, numbers, hyphens, and periods can be used in a domain name.* *Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.*
***DYNDNS**	Query or set the Dynamic DNS Service type to use. AT*DYNDNS? to query AT*DNYDNS=n to set • n=0—Disable (default) • n=2—dyndns.org • n=5—noip.org • n=6—ods.org • n=8—regfish.com • n=9—tzo.org • n=10—IP Manager *Note: Only IP Manager can be fully configured using AT Commands.*
***IPMANAGER1** ***IPMANAGER2**	*Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.* Query or set a FQDN or IP address of the IP server to send IP change notifications to. You can configure two independent IP Manager servers. AT*IPMANAGER[n]? to query AT*IPMANAGER[n]=SERVER to set. • n=1—First IP Manager server • n=2—Second IP Manager server • SERVER = Server FQDN or IP address Note: You can disable updates to a server by setting blank entry (e.g., “AT*IPMANAGER1=”).

Table C-6: Services AT Commands (Continued)

Command	Description
***IPMGRKEY1** ***IPMGRKEY2**	*Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.* Query or set the 128-bit password/key used to authenticate the IP update notifications. If the key's value is all zeros, a default key is used. If all the bytes in the key are set to FF, then no key is used (i.e., the IP change notifications will not be authenticated). AT*IPMGRKEY[n]? to query AT*IPMANAGER[n]=KEY to set • n=1—First IP Manager server • n=2—Second IP Manager server • KEY=128-bit key in hexadecimal [32 hex characters]
***IPMGRUPDATE1** ***IPMGRUPDATE2**	*Note: This AT command is only usable if the Dynamic DNS Service type is set to IP Manager.* Query or set the interval (in minutes) to send an IP update notification to the corresponding server. This occurs even if the IP address of the device does not change. If the value is set to 0, then periodic updates are not issued (i.e., IP change notifications is only be sent when the IP actually changes). AT*IPMGRUPDATE[n] to query AT*IPMGRUPDATE[n]=INTERVAL to set • n=0—Disables the update interval (updates only on changes) • n=1—First IP Manager server • n=2—Second IP Manager server • INTERVAL=1–255—interval (in minutes) to send an update
***MODEMNAME**	*Note: This AT command is only usable if AT*DYNDNS is set to 10 (IP Manager).* Query or set the device name used by IP Manager. (This name is displayed on the Status > Home page.) AT*MODEMNAME? to query AT*MODEMNAME=NAME to set (up to 20 characters long) • NAME= device name (for example, mydevice) The value in *DOMAIN provides the domain zone to add to this name. Example: If *MODEMNAME=mydevice and *DOMAIN=eairlink.com, the device's fully qualified domain name is mydevice.eairlink.com. **Tip:** *Each device using IP Manager needs a unique name. I.e., two devices cannot both be called "mydevice". One could be named "mydevice1" while the other could be named "mydevice2".*

Table C-6: Services AT Commands (Continued)

Command	Description
SMS	

***SMSM2M**
***SMSM2M_8**
***SMSM2M_u**
	You can only use these commands locally.
	• AT*SMSM2M sends an SMS in ASCII text (requires quotation marks; maximum 140 characters)
	• AT*SMSM2M_8 sends an 8-bit SMS (requires quotation marks; maximum 140 characters)
	• AT*SMSM2M_U sends a unicode SMS (requires quotation marks; maximum 140 characters)
	Format:
	AT*SMSM2M="[phone] [ascii message]"
	AT*SMSM2M_8="[phone] [hex message]"
	AT*SMSM2M_U="[phone] [hex message]"
	• The phone number can only consist of numbers (NO spaces or other characters). The phone number should be as it appears in the Last Incoming Phone Number field.
	  • Example 1 (US): 14085551212 (including leading 1 and area code)
	  • Example 2 (US): 4085551212 (ignore leading 1, include area code)
	  • Example 3 (UK): 447786111717 (remove leading 0 and add country code)
	Command Examples:
	AT*SMSM2M="18005551212 THIS IS A TEST" sends in ASCII.
	AT*SMSM2M_8="17604053757 544849532049532041205445535 4" sends the message "THIS IS A TEST" as 8-bit data.
	AT*SMSM2M_U="17604053757 000102030405060708090a0b0c0d0e0f808182838485868788898A8b8c8d8e8f" sends the bytes:
	00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f
	80 81 82 83 84 85 86 87 88 89 8a 8b 8c 8d 8e 8f
	Note: Not all cellular Mobile Network Operators support 8-bit or unicode SMS messages.

***SMS_PASSWORD**	Query or set the SMS password. AT*SMS_PASSWORD? to query AT*SMS_PASSWORD=n n=SMS password If no password has ever been configured, a default password is created from the last four characters of the SIM ID (for all SIM-based devices) or the ESN (for devices without a SIM, such as those using EV-DO). *Note: The configured password remains in place, even when the device is reset to factory default settings.*

Table C-6: Services AT Commands (Continued)

Command	Description
***SMSWUPTOUT**	This AT Command only to International devices on the Vodafone network. Query or set the connection timeout for the SMS Wakeup feature. When this feature is enabled, an IP connection is initiated on receipt of a specific type of SMS (For information on choosing the type of SMS, see Services > SMS > SMS Wakeup > SMS Wakeup Trigger described in step 3 on page 161). The IP connection closes after the timeout period specified in this AT command. Outgoing traffic sent after the timer is set does not reset the timer. AT*SMSWUPTOUT? to query AT*SMSWUPTOUT=n to set • n=2–65535 minutes (default is 2) See also *RADIO_CONNECT on page 295.
Telnet/SSH	
***DEFAULTTELNETUSER**	Query or set the Telnet default user name AT*DEFAULTTELNETUSER? to query AT*DEFAULTTELNETUSER=n to set • n=None—Prompted for a user name and password when logging into a Telnet session (default) • n=user—Prompted for a password only when logging into a Telnet session (User name is “user”.) *Note: The default user name is only for Telnet; not SSH.*
***TELNETTIMEOUT**	Query or set the Telnet/SSH idle time out. By default, this value is set to close the telnet/SSH connection if no data is received for 2 minutes. AT*TELNETTIMEOUT? to query AT*TELNETTIMEOUT=n to set • n=1–255 minutes (Default is 2.)
***TSSH**	Query or set the remote login server mode. AT*TSSH? to query AT*TSSH=n to set • n=0—Telnet (default) • n=1—SSH
***TPORT**	Query or set the Telnet/SSH port. AT*PORT? to query AT*PORT=n to set • n=1–65535 (Default is 2332.) Many networks have the ports below 1024 blocked. It is recommended to use a higher numbered port.
***TQUIT**	AT*TQUIT which will kill an open telnet session to the LS300 device.

Table C-6: Services AT Commands (Continued)

Command	Description
Management (SNMP)	
SNMP General Configuration	
***SNMP**	Query or set the SNMP option. AT*SNMP? to query AT*SNMP=n to set • n=0—Disable • n=1—Enable
***SNMPCONTACT**	Add string contact information in SNMPv2 and SNMPv3. AT*SNMPCONTACT=string • string=email address (Example: admin@sierrawireless.com)
***SNMPLOCATION**	Add string location information in SNMPv2 and SNMPv3. AT*SNMPLOCATION=string • string=location information (Example: Building 19–67B)
***SNMPNAME**	Add string name in SNMPv2 and SNMPv3. AT*SNMPNAME=STRING • STRING=name (Example: John Doe)
***SNMPPORT**	Query or set the port number in SNMPv2 and SNMPv3. AT*SNMPPORT? to query AT*SNMPPORT=n to set • n=1–65535 (Default is 161.)
***SNMPVERSION**	Query or set the SNMP version. AT*SNMPVERSION? to query AT*SNMPVERSION=n to set • n=2—version 2 • n=3—version 3
SNMP Read Only Configuration	
***SNMPROCOMMUNITY**	Read-only community string in SNMPv2 and SNMPv3 (SNMP equivalent of a password; for example: public)
***SNMPROUSER**	Query or set a read only SNMP username string in SNMPv3.
***SNMPROUSERAUTHTYPE**	Query or set the read only authentication type in SNMPv3. AT*SNMPROUSERAUTHTYPE? to query AT*SNMPROUSERAUTHTYPE=n • n=0—MD5 • n=1—SHA

Table C-6: Services AT Commands (Continued)

Command	Description
***SNMPROUSERSECLVL**	Query or set the read only security level in SNMPv3. AT*SNMPROUSERSECLVL? to query AT*SNMPROUSERSECLVL=n to set • n=0—none • n=1—authentication only • n=2—authentication + privacy
SNMP Read/Write Configuration	
***SNMPRWCOMMUNITY**	Read/write community string in SNMPv2 and SNMPv3. (SNMP equivalent of a password; for example: private)
***SNMPRWUSER**	Query or set a read/write SNMP username string in SNMPv2 and SNMPv3.
***SNMPRWUSERAUTHTYPE**	Query or set the read/write authentication type in SNMPv3. AT*SNMPRWUSERAUTHTYPE? to query AT*SNMPRWUSERAUTHTYPE=n to set • n=0—MD5 • n=1—SHA
***SNMPRWUSERSECLVL**	Query or set the read/write security level in SNMPv3. AT*SNMPRWUSERSECLVL? to query AT*SNMPRWUSERSECLVL=n to set • n=0—none • n=1—authentication only • n=2—authentication + privacy
***SNMPRWUSERPRIVTYPE**	Query or set the read/write privacy type in SNMPv3. AT*SNMPRWUSERPRIVTYPE? to query AT*SNMPRWUSERPRIVTYPE=n to set • n=0—DES • n=1—AES
SNMP TRAP Configuration	
***SNMPENGINEID**	Specify an identification name string for a SNMP engine in SNMPv3. (For example: Shark-0012E8)
***SNMPTRAPAUTHTYPE**	Query or set the SNMP TRAP authentication type in SNMPv3. AT*SNMPTRAPAUTHTYPE? to query AT*SNMPTRAPAUTHTYPE=n to set • n=0—MD5 • n=1—SHA
***SNMPTRAPCOMMUNITY**	SNMP TRAP community string in SNMPv2 and SNMPv3. (SNMP equivalent of a password)
***SNMPTRAPDEST**	Query or set the SNMP TRAP destination in SNMPv2 and SNMPv3. (for example: 192.168.13.33)
***SNMPTRAPPORT**	• Query or set the SNMP TRAP port in SNMPv2 and SNMPv3. 1–65535 (Default is 162.)

Table C-6: Services AT Commands (Continued)

Command	Description
***SNMPTRAPPRIVTYPE**	Query or set the SNMP TRAP privacy type in SNMPv3. AT*SNMPTRAPPRIVTYPE? to query AT*SNMPTRAPPRIVTYPE=n to set • n=0—DES • n=1—AES
***SNMPTRAPSECLVL**	Query or set the SNMP TRAP security level in SNMPv3. AT*SNMPTRAPSECLVL? to query AT*SNMPTRAPSECLVL=n to set • n=0—none • n=1—authentication only • n=2—authentication + privacy
***SNMPTRAPUSER**	Query or set a SNMP TRAP username string in SNMPv3.
Email (SMTP) Commands	
***SMTPADDR**	Query or set the mail server IP address or FQDN. AT*SMTPADDR? to query AT*SMTPADDR=[d.d.d.d] or [NAME] to set • d.d.d.d=IP Address • NAME=domain name (maximum: 40 characters)
***SMTPFROM**	Query or set the email address from which the SMTP message is being sent (required by some mail servers). AT*SMTPFROM? to query AT*SMTPFROM=EMAIL to set • EMAIL=email address (maximum: 30 characters)
***SMTPSUBJ**	Query or set the email subject line to use for sending emails. AT*SMTPSUBJ? to query AT*SMTPSUBJ=STRING to set
***SMTPPW**	Query or set the email server password (required by some mail servers). AT*SMTPPW? to query AT*SMTPPW=PASSWORD to set
***SMTPUSER**	Query or set the email account username (required by some mail servers). AT*SMTPUSER? to query AT*SMTPUSER=USER to set (maximum: 40 characters)

Table C-6: Services AT Commands (Continued)

Command	Description
Time (SNTP) Commands	
***SNTP**	Query or set daily SNTP updates of the system time. AT*SNTP? to query AT*SNTP=n to set • n=0—Off • n=1—On
***SNTPADDR**	SNTP Server IP address, or fully-qualified domain name, to use if *SNTP=1. AT*SNTPADDR? to query AT*SNTPADDR=[d.d.d.d] or [NAME] • d.d.d.d=IP Address • NAME=FQDN

Serial

Table C-7: Serial AT Commands

Command	Description
AIP	Query or set the option to allow IP addresses to communicate on UDP over serial. AT*AIP? to query AT*AIP=n to set • n=0—Allow only the IP address specified in S53 to connect when UDP auto answer is enabled (S82=2) • n=1—Allow any incoming IP address to connect when UDP auto answer is enabled (S82=2) Always subject to any security filters that may be defined. (See Security on page 304.)
\APPP	Initiates a PPP connection on serial terminal. You can also initiate a PPP connection using the ADT command and one of the supported phone numbers.
***CTSE**	Query or set asserting Clear To Send (CTS) when there is a network coverage. AT*CTSE? to query AT*CTSE=n to set • n=0—Disabled (default) • n=1—Enable assertion of CTS when there is network coverage
DAE	Query or set AT Escape Sequence detection. ATDAE? to query ATDAE=n to set • n=0—Enable • n=1—Disable (The escape sequence (+++) is ignored.)

Table C-7: Serial AT Commands (Continued)

Command	Description
***DEVPPP**	Query or configure the gateway's IP address for Point to Point Protocol (PPP). AT*DEVPPP? to query AT*DEVPPP=x.x.x.x to configure, where x.x.x.x is the IP address for the AirLink gateway. To configure the host IP address for PPP, see *HOSTPPP on page 314.
***DPORT**	Query or set the device port that the device listens on for inbound packets/data/polls. AT*DPORT? to query AT*DPORT=n to set • n=1–65535
***DU**	Query or set the dial command to only use UDP. AT*DU? to query AT*DU=n to set • n=0—Dial using the means specified (default) • n=1—Dial UDP always, even when using ATDT When this parameter is set you cannot establish a TCP PAD connection by using the Dial command.
***ENQ**	Query or set the option to output an ENQ [0x05] after the TCP CONNECT, delayed by the Delay Connect Response time (S221). AT*ENQ? to query AT*ENQ=n to set • n=0—Disable (default) • n=1—Enable ENQ on TCP CONNECT
***HOSTPPP**	Query or configure the host's IP address for Point to Point Protocol (PPP). AT*HOSTPPP? to query AT*HOSTPPP=x.x.x.x to configure, where x.x.x.x is the IP address for the host computer. To configure the gateway's IP address for PPP, see *DEVPPP on page 314.
***HOSTMODE?**	Query the current host mode. AT*HOSTMODE? returns: • AT • PPP • TCP • UDP *Note: If the device is not in AT mode, Telnet into the device to execute this command.*

Table C-7: Serial AT Commands (Continued)

Command	Description
MD	Query or set the default start-up mode for the serial port. When the device is power-cycled, the serial port enters the mode specified by this command after 5 seconds. On startup, typing ATMD0 within 5 seconds changes the mode to normal (AT command) mode. See also S53 to set the port for UDP. AT*MD? to query AT*MD=hh to set • hh (hex byte)=00 — Normal (AT Command mode) • hh=02 — PPP • hh=03 — UDP • hh=04 — TCP • hh=08 — reverse telnet/ssh • hh=83 — UDP Multiple Unicast
IPL	Query or set the IP list dial. AT*IPL? to query AT*IPL=n to set • n=0—Disable • n=1—Enable This allows you to access to the Modbus IP address list using the first two digits of the dial string. Example: ATDT1234567 would go to ID “12” on the Modbus list and use the associated IP as the destination.
***NUMTOIP**	Query or set the option to convert a 12-digit number to an IP address For example, converts 111222333444 to 111.222.333.444 AT*NUMTOIP? to query AT*NUMTOIP=n to set • n=0—Disable • n=1—Enable
S50	Query or set the data forwarding idle timeout. ATS50? to query ATS50=n to set • n=0—a forwarding timeout of 10ms is used. • n= tenths of a second
S51	Query or set the PAD data forwarding character. ASCII code of character that causes data to be forwarded. Used in UDP or TCP PAD mode. ATS51? to query AT51=CHARACTER to set • n=0—No forwarding character • n=CHARACTER

Table C-7: Serial AT Commands (Continued)

Command	Description
S53	Query or set the method (dial mode), destination IP address, and port used as defaults for the D (Dial) AT command. ATS53? to query ATS53=[method][d.d.d.d][/ppppp] to set [method] can be: • P—UDP • T—TCP [d.d.d.d] is the destination IP address [pppp] is the port number. Example: ATS53=P111.22.33.44/5555 where: • The first character is the dial mode (P in this example) • Followed by destination IP address (111.22.33.44 in this example) • A slash • Followed by the destination port (5555 in this example) You can also use this command to set only the port. For example, AT53=/7777.
S60	Query or set the Telnet Client Echo Mode. ATS60? to query ATS60=n to set • n=0—No Echo • n=1—Local Echo (default) • n=2—Remote Echo
S82	Query or set UDP auto answer. ATS82? to query ATS82=n to set • n=0—Disable • n=1—Enable
S83	Query or set the UDP auto answer idle timeout. If no data is sent or received before the timeout occurs, the current UDP session is terminated. While a session is active, packets from other IP addresses are discarded (unless *UALL is set). ATS83? to query ATS83=n to set • n=0—No idle timeout (default) • n=1–255—Timeout in seconds
***SERIALLEDDISPLAY**	Query or set whether or not the Activity LED on the AirLink gateway indicates traffic on the selected serial port. AT*SERIALLEDDISPLAY? to query AT*SERIALLEDDISPLAY=n to set • n=0—LED display of serial traffic disabled (default) • n=1—LED display of serial traffic enabled For a description of the Activity LED when this parameter is enabled, see Display on page 211.

Table C-7: Serial AT Commands (Continued)

Command	Description
***SERIALLEDPORT**	Query or set the serial port that the Activity LED indicates traffic on if AT*SERIALLEDDISPLAY is set to 1. AT*SERIALLEDPORT? to query AT*SERIALLEDPORT=n to set • n=0—Main serial port on the AirLink gateway itself (default) • n=1—Serial port on the I/O X-Card (applies only to an AirLink GX Series gateway with an I/O X-Card installed)
TCPS	Query or set the TCP connection time-out (TCPS) units. If there is no traffic through the TCP connection for the specified interval, the connection is terminated. AT*TCPS? to query AT*TCPS=n to set • n=0—minutes • n=1—seconds
TCPT	Query or set the interval to terminate a TCP connection when there is no traffic. This value affects only the TCP connection in TCP PAD mode. AT*TCPT? to query AT*TCPT=n to set • n=0–255
***UALL**	Query or set the ability to accept UDP packets from any IP address when a UDP session is active. If there is no UDP session active, an incoming UDP packet will be treated according to the UDP auto answer and AIP settings. AT*UALL? to query AT*UALL=n to set • n=0—No effect (default) • n=1—Accept UDP data from all IP addresses when in a UDP session
***UDPLAST**	Query or set the option to set S53 to the last accepted IP address through UDP auto answer. This can be used in conjunction with MD3 so that when there is no UDP session, new Ethernet host data will cause a connection to be restored to the last IP accepted through UDP auto answer. AT*UDPLAST? to query AT*UDPLAST=n to set • n=0—Does not change destination IP (default) • n=1—Change destination IP to last received
***UDPPADMTU**	Query or set the size of serial MTU (PAD payload) AT*UDPPADMTU? to query AT*UDPPADMTU=n to set • n=256–4096
***USD**	Query or set the specified delay before sending the UDP packets out the serial port. AT*USD? to query AT*USD=n to set • n=0—No UDP packet delay (default) • n=1–255—Delay in 100ms units, from 100 ms to 25.5 sec.

Standard (Hayes) commands

The following table contains Hayes commands supported on AirLink gateways.

Table C-8: Standard (Hayes) AT Commands

Command	Description
+++	AT escape sequence (not preceded by AT) If a serial terminal is in a data mode, typing this sequence on that serial terminal causes the terminal to re-enter AT command mode. There must be an idle time on the serial port before and after the sequence. The idle time is set by the value in S50. After you type the AT escape sequence, the terminal remains in AT command mode for 15 seconds before it automatically leaves AT command mode and returns to the previous data mode. *Note: The "+" is ASCII character 0x2B.* *Note: The detection of this sequence is disabled if DAE=1.*
&C	Query or set Data Carrier Detect (DCD) mode. DCD is a hardware signal that notifies the software that the device is communicating with another device. AT&C? to query AT&Cn to set • n=0—Always assert DCD • n=1—Assert DCD enable when network is ready (default) *Note: Do not use an equal sign (=) when issuing the command.*

Table C-8: Standard (Hayes) AT Commands (Continued)

Command	Description
D[*method*] [*d.d.d.d*] [*/ppppp*] or D[*method*] [[@]*name*] [*/ppppp*]	Dial a connection to a remote IP and Port using either UDP, TCP, or Telnet. You can only use ATD#19788 and ATDT#19788 locally. *method* = P—Establish a UDP connection T—Establish a TCP connection N—Establish a Telnet connection *d.d.d.d* = IP address to establish connection to *name* = Domain name to establish connection to *ppppp* = IP port to establish connection to Examples: **ATD**—Dial (establish) default connection per **S53** **ATDP***nnn.nnn.nnn.nnn*[/ppppp]—Dial (establish) UDP session to the specified IP address/port. If the method, IP address, or port is omitted, the values from S53 are used. If a Telnet connection is requested (N) and the port is not supplied, port 23 will be used instead of the value from S53. Several special dialing numbers exist to make it easy to establish a **PPP** connection with the device. **ATD#19788** or **ATDT#19788** will establish a PPP connection (see \APPP on page 313). If a domain name is specified, the '@' symbol can be used to explicitly indicate the start of the name. For example, if "**ATDPHONY**" is issued, this will be interpreted as dial a UDP connection to "HONY". To dial using the default method to host "PHONY", one would issue "ATD@PHONY". To end the connection, issue the **+++** escape sequence or drop the DTR line (if Ignore DTR **S211=0** or **&D2**). *Note: The source port of the session is the **Device Port** (set by ***DPORT**).*
&D	Query or set Data Terminal Ready (DTR) mode. AT&D? to query AT&Dn to set • n=0—Devices ignores DTR, same effect as HW DTR always asserted (same as S211=1); DTD is assumed to be on. • n=1—DRT drop causes the device to switch to AT command mode, but does not drop the connection. • n=2—DTR drop causes the connection to drop. • n=3—DTR drop causes the connection to reinitialize. *Note: Do not use an equal sign (=) when issuing the command.*
***DATZ**	Query or set the option to block device reset using ATZ. AT*DATZ? to query AT*DATZ=n to set • n=0—Off. Block is disabled—ATZ resets the device. (default) • n=1—On. Block is enabled—ATZ does not reset the device.

Table C-8: Standard (Hayes) AT Commands (Continued)

Command	Description
E	Toggle AT command echo mode. ATE? to query ATEn to set • n=0—Echo Off; does not echo commands to the computer • n=1—Echo On; echoes commands to the computer (so you can see what you type) *Note: Do not use an equal sign (=) when issuing the command.*
H	ATH hangs up, immediately terminates the session (PAD or PPP).
HOR	Half-Open Response—In UDP auto answer (half-open) mode. AT*HOR? to query AT*HOR=n to set • n=0—No response codes when UDP session is initiated • n=1—RING CONNECT response codes sent out serial link before the data from the first UDP packet *Note: Quiet Mode must be Off.*
Q	Query or set AT quiet mode. If quiet mode is set, there is no responses to AT commands except for data queried. ATQ? to query ATQn to set • n=0—Off (default) • n=1—Quiet mode on *Note: Do not use an equal sign (=) when issuing the command.*
\Q	Query or set the serial port flow control. AT\Q? to query AT\Qn to set • n=0—No flow control • n=1—Hardware flow control • n=4—Transparent software flow control *Note: Do not use an equal sign (=) when issuing the command.*
&S	Query or set DSR. AT&S? to query AT&Sn to set • n=0—Always assert • n=1—Assert DSR while in data mode (UDP, TCP, PPP) *Note: Do not use an equal sign (=) when issuing the command.*

Table C-8: Standard (Hayes) AT Commands (Continued)

Command	Description
S0	Query or set TCP auto answer (the number of rings required before the device automatically answers a call). ATS0? to query ATS0n to set • n=0—Disable • n=1—Enable *Note: Do not use an equal sign (=) when issuing the command.*

Table C-8: Standard (Hayes) AT Commands (Continued)

Command	Description
S23	Query or set the Serial port configuration *Note: The serial port parameter is optional. If no serial port is specified, ATS23 queries or sets the serial port it is received on.* ATS23?[Serial port] to query • 0=Serial port on the device • 1=Serial port on the I/O X-Card, if installed on a GX device ATS23=[Baud,][Data bits, Parity, Stop Bits][,Serial port] to set Baud: • 300 • 1200 • 2400 • 4800 • 9600 • 19200 • 38400 • 57600 • 115200 Data bits: • 7 • 8 Parity: • O=Odd • E=Even • N=None • M=Mark Stop Bits: • 1 • 1.5 • 2 Serial port: • 0=Serial port on the device • 1=Serial port on the I/O X-Card, if installed on a GX device Example: ATS23=115200,8,N,2,0 (Sets the device to 115200, etc.) The settings take effect after reboot. *Note: Must be 8 data bits for PPP mode.*

Table C-8: Standard (Hayes) AT Commands (Continued)

Command	Description
S211	For applications or situations where hardware control of the DTR signal is not possible, the device can be configured to ignore DTR. When Ignore DTR is enabled, the device operates as if the DTR signal is always asserted. ATS211? to query ATS211=n to set • n=0—Use hardware DTR (default) • n=1—Ignore DTR • n=3—Ignore DTR and assert DSR.
S221	Query or set the Connect Delay—the number of seconds to delay the connect response when establishing a TCP connection. ATS211? to query ATS211=n to set • n=0–255
V	Query or set the AT command responses (verbosity). ATV? to query ATVn to set • n=0—Numeric (terse) command responses (The numeric responses follow the Hayes Standards for commands.) • n=1—Text string (verbose) command responses (default) *Note: Do not use an equal sign (=) when issuing the command.*
&V	Lists most AT commands and their current values. If the parameter is not configured, the AT command returns “Not Set”.
&W	Saves the settings for parameters that are temporarily set without being permanently written to the memory. This command does not apply to ALEOS because once you issue an AT command or change a setting in ACEmanager and click Apply, the changes are saved in non-volatile memory and persist across reboots.
X	Query or set the Extended Call Process Result mode ATX? to query ATXn to set • n=0—No extended code (default) • n=1—Adds the text 19200 to the connect response
Z	Reboots the AirLink gateway. *Note: If *DATZ is set to 1, Z is blocked. See *DATZ on page 319.*

I/O

Table C-9: Input/Output AT Commands

<table>
<tr><th>Command</th><th>Description</th></tr>
<tr><td>*DIGITALIN1?</td><td>Query individual digital inputs. The digital inputs report either a 0 (open) or 1 (closed).
AT*DIGITALIN1?
• Digital 1 is the on-board digital input.

<table><tr><th>Volts</th><th>Digital value</th></tr><tr><td>-0.5 – 1.2</td><td>0</td></tr><tr><td>1.3 – 30</td><td>1</td></tr></table></td></tr>
<tr><td>*PULSECNT1?</td><td>Query the I/O pulse counts for digital in.
AT*PULSECNT1?</td></tr>
<tr><td>*RELAYOUT1</td><td>Query or set the relay status.
AT*RELAYOUT1? to query
AT*RELAYOUT1=n to set
• n=0—OFF
• n=1—Drive Active Low</td></tr>
</table>

Applications

Table C-10: Applications > Data Usage Commands

Command	Description
***DATACURDAY?**	Display data usage for the current day (in KB).
***DATAPLANUNITS**	Query or set the units for the data usage report AT*DATAPLANUNITS to query AT*DATAPLANUNITS=n to set • n=1—Sets the units to Megabytes (MB) • n=2—Sets the units to Kilobytes (KB)
***DATAPREVDAY?**	Query the data usage for the previous day (in KB).
***DATAUSAGEENABLE**	Query or set enabling Data Usage. AT*DATAUSAGEENABLE? to query AT*DATAUSAGEENABLE=n to set • n=0—Data Usage disabled • n=1—Data Usage enabled

Table C-11: Applications > ALEOS Application Framework (AAF)

Command	Description
***AAFINSTALL**	Query installed AAF applications and their status and install new AAF applications • AT*AAFINSTALL? returns the installation status of the last installed application, and list of installed AAF applications and the status of each application. • AT*AAFINSTALL?<application name> returns the status of the specified AAF application. • AT*AAFINSTALL=<hostname>,<user>,<password>,<application filename> downloads and installs the specified AAF application from the FTP server at <hostname> using <user> <password> credentials.
***AAFUNINSTALL**	Install an AAF application AT*AAFUNINSTALL=<application name> uninstalls the specified AAF application.

Admin

Table C-12: Admin > Advanced Commands

Command	Description
\ACEPW	Set the ACEmanager user password remotely. AT\ACEPW=<password> to set • <password>=character string The password can be 4 to 32 characters long and can contain a mixture of letters, numbers, and/or special characters. The password is case sensitive. To change the password, send the AT Command. You will not be asked to re-enter or confirm the new password. *Note: If the password is lost, the only way to recover access to the AirLink gateway is to use the hardware reset button to reset the device to the factory default settings. If the reset button has been disabled (using the Default Configuration Reset field on the Admin > Advanced screen) prior to the password being lost, the only way to recover access to the AirLink gateway is through AirVantage Management Services, for which an account is required.*
***BLOCK_RESET_CONFIG**	Query or set the ability to block resetting the device to factory default settings using the hardware Reset button. AT*BLOCK_RESET_CONFIG? to query AT*BLOCK_RESET_CONFIG=n to set • n=0—Reset button can be used to reset the device to factory default settings. (default). • n=1—Device cannot be reset to factory default settings using the Reset button on the device. *Note: This command only blocks the ability to reset to defaults using the Reset button on the device. You can still reset the device to the factory default settings using the "Reset to Factory Default" button in ACEmanager or the *RESETCFG AT command.*
***BOARDTEMP?**	Query the temperature of the internal hardware, in degrees Celsius.

Table C-12: Admin > Advanced Commands (Continued)

Command	Description
***DATE?**	Query the internal clock. The date and time are always specified in a 24-hour notation. AT*DATE? to query
***MSCIUPADDR**	Query or set the IP address or FQDN and port that periodic device status updates are sent to. AT*MSCIUPADDR[IP address or FQDN][/port]? to query AT*MSCIUPADDR=[IP address or FQDN][/port] to set Examples: 192.168.14.100/3333 MyDevice.com/3333
***MSCIUPDPERIOD**	Query or set the device status update interval (in seconds). Thsi specifies how frequently the device status update is sent to the port configured in *MSCIUPADDR. AT*MSCIUPDPERIOD? to query AT*MSCIUPDPERIOD=n to set • n=0—Disabled • n=1–255 seconds
NSLOOKUP	Immediately performs an NSLookup on the supplied FQDN. ATNSLOOKUP=[FQDN]
***POWERIN?**	Query the voltage input to the internal hardware.
***RESETCFG**	AT*RESTCFG resets the device to factory default settings. **Important:** *There is no confirmation requested. The AT command takes effect immediately.*
***REMOTELOG**	Exports the log file to a remote destination (Syslog Server). Specifying the port is option. If the port is not specified, the default port, 514, is used. You can only use this command locally. AT*REMOTELOG=SYSLOG SERVER IP,PORT

Table C-12: Admin > Advanced Commands (Continued)

Command	Description

***SECUREMODE**	Query or set the secure mode that blocks most ports (and ICMP) for over-the-air (OTA) or OTA and local to prevent unwanted access to the device.
	AT*SECUREMODE? to query
	AT*SECUREMODE=n to set
	• n=0—Off; normal behavior
	• n=1—Disables:
	  • Web management ports (ACEmanager and AVMS access) from the OTA interface
	  • Internet Control Message Protocol (ICMP), used for PING, for OTA and Wi-Fi
	• n=2—Disables:
	  • Web management ports from the Over-the-air (OTA) interface
	  • Internet Control Message Protocol (ICMP) for OTA and Wi-Fi
	  • ICMP for local ports (Ethernet, USB, and Serial)
	Note: Telnet and SSH ALEOS ports remain open regardless of the secure mode setting. This enables you to connect an AT console to manage the device. DHCP and DNS ports also remain open to allow the device to provide IP addresses to hosts and relay the DNS service.

***SYSRESETS?**	Query the number of resets since the device was reset to factory default settings.
***USBBYPASS**	Query or set Radio Passthru mode. AT*USBBYPASS? to query AT*USBBYPASS=n to set • n=0—Disable • n=1—Enable

D: SMS Commands

SMS Command format

PW [Password] [Prefix][Command or Command parameter1] [Command parameter2 (if applicable)] [Command parameter n]

Note: There is no space between the prefix and the command (or the 1st command parameter in the case of multi-parameter commands). There must be a single space between all other fields to act as a delimiter.

The default password is the last 4 digits of the SIM ID number (for SIM-based devices) and the last 4 digits of the ESN (for non-SIM devices). If you do not know the SIM ID or ESN number, you can find it in ACEmanager on the Status > WAN/Cellular page.

The default prefix is “&&&”.

Whether or not a password and prefix are required varies depending on the SMS mode selected in ACEmanager.

SMS mode	Password (configurable in all modes)	Prefix
Password Only	Always required	Required Use default (not configurable)
Control Only	Required when sending from a non-trusted phone number	Prefix is configurable. The prefix can be omitted if the ALEOS Command Prefix field in ACEmanager (Services > SMS) is configured to be blank.
Gateway Only	Always required	Required Use default (not configurable)
Control and Gateway	Required when sending from a non-trusted phone number	Required Configurable, but cannot be blank

When an SMS command is received, the AirLink gateway performs the action requested and sends a response back to the phone number from which it received the SMS.

For more examples and detailed instructions, see SMS Overview on page 149.

List of SMS Commands

Command	Action	Result
Note: Some responses start with "reply from [device name]:" However, this feature is currently unavailable for the Enable, and Provision commands.		
[prefix]enable <value>	Enable/disable the device(s) being managed by AVMS.	"AVMS enable set to status:" <value> <value>=0 Disable <value>=1 Enable
[prefix]status	None	status IP [Network IP] [Network Status]: [technology type] RSS signalled Lat = [Latitude] Long = [Longitude] Time = [hh:mm:ss]
[prefix]reset	Resets the device 30 seconds after the first response message is sent.	First message: Reset in 30 seconds Second message: Status message when back up.
[prefix]relay x y	Sets the applicable relay to the desired setting.	relay x set to y x can be 1 y can be 0 or 1 (Off or Drive active low)
[prefix]Provision <APN> <Network User ID> <Network Password> <Network Authentication Mode> *Note: You can omit any of the above parameters.* • *To omit a parameter before the one you want to change, use a period (.) in place of the omitted parameter. Example: &&&provision . user@carrier.com . chap changes only the user ID and authentication mode.* • *If you want to omit any parameters after the one you want to change, simply omit them. Example: &&&provision access.apn changes only the apn.* *Note: Use of this command is valid for LTE, HSPA, and GPRS networks, but not valid for CDMA only networks.*	After the unit is installed and the SIM card inserted, you can use this command to provision the account. Network Authentication Mode is optional. If used, enter one of the following: • None • PAP • CHAP These are not case sensitive. If an unknown mode is entered or the field is omitted, None is used.	"provision" "apn:" <APN> "user ID" <Network User ID> "PW" <Network Password> "auth mode" <Network Authentication Mode> *Note: If a parameter is omitted, the response displays "Not Set" for that parameter.*

Command	Action	Result
[prefix]AVMS <server> <interval> *Note: All of the above must be on a single line. The interval must be greater than 0. Omitting any field results in a response of "not set" and the configuration parameter does not change.*	Modifies the AVMS server's URL and AVMS communication period (interval in minutes)	"AVMS" "srv:" <Server> "interval:" <Interval>
[prefix]AVMSCHECKIN	Prompts the device to communicate with the AVMS server. Once AirVantage Management Service receives the heartbeat message, it can respond and send an MSCI command to the device (i.e Write/Read/ Firmware Update).	"AVMS connection requested"

E: Q & A and Troubleshooting

ACEmanager Web UI

The ACEmanager page is not displaying properly.

1. Ensure that you are using a supported browser. See page 12 for a list of supported browsers.
2. Hold the Shift key + click the Refresh button. This reloads the page, while ignoring what is in the cache.

If the problem persists:

- Clear the cache. (The procedure varies, depending on the browser.)
- Restart the browser.
- Restart your computer.

Ethernet Ports

What do the LEDs above the Ethernet port mean?

There are two LEDs at the top of the Ethernet port. The green on is lit when there is a cable connected to the host and the connection is running at 100baseT. The amber (activity) LED blinks when traffic is passing through the port.

LAN Networks

The server on my LAN network is receiving data from some hosts on the network, but not others. What's wrong?

If you have a network with multiple LAN hosts that are sending data to the same server and the server is not receiving data from one (or more) of the hosts, it may be because the Mobile Network Operator has a WAN firewall that is blocking the ports used by the NAT for over-the-air (OTA) destinations.

To correct this problem:

1. Launch ACEmanager.
2. Go to the LAN tab.
3. Select Ethernet.
4. Refer to the instructions for setting the Starting Ephemeral Port on page 90.)

Port Forwarding

I set up port forwarding rules. I did not receive an error message, but it seems that data is not being forwarded.

If the Public Start Port and Public End Port fields are not set up correctly, data is not forwarded.

1. In ACEmanager, go to Security > Port Forwarding.

- If you are forwarding data to a single port:
  - Ensure that the value in the Public Start Port field is **not** 0.
  - Ensure that the value in the Public End Port field **is** 0.
  - Ensure that the value in the Private Port start field is **not** 0.
- If you are forwarding data to a range of ports:

1. Ensure that the value in the Public Start Port field is not 0.
   - Ensure that the value in the Public End Port field is greater than the value in Public Start Port field.
   - Ensure that the value in the Private Port Start field is not 0.

For complete instructions, see Port Forwarding on page 126.

ALEOS Application Framework (AAF)

I'm unable to load an application from AAF.

1. In ACEmanager, go to Services > Telnet/SSH.
2. In the AT Server Mode field, select Telnet.
3. Click Apply.
4. Re-try loading the application from AAF.

SMS

I tried to send an SMS message, and received an error code. What does the error code mean?

The following acknowledgment error codes may appear if your message was not successfully sent:

Code:	Explanation:
100	Not in coverage (no cellular service)
201	Parse Error on field #1 (Start Field)
202	Parse Error on field #2 (Phone number and separator)
203	Parse Error on field #3 (Data type and separator)
204	Parse Error on field #4 (Payload length and separator)
205	Parse Error on field #5 (Message and End Field)
301	No buffers available
302	SMS queue full

Supported SMS data types are ASCII, 8-bit, and Unicode, and are all case-sensitive. SMS messages being sent MUST be in ASCII hex format.

I tried to send an SMS command and received the error "not set". The parameter was not changed.

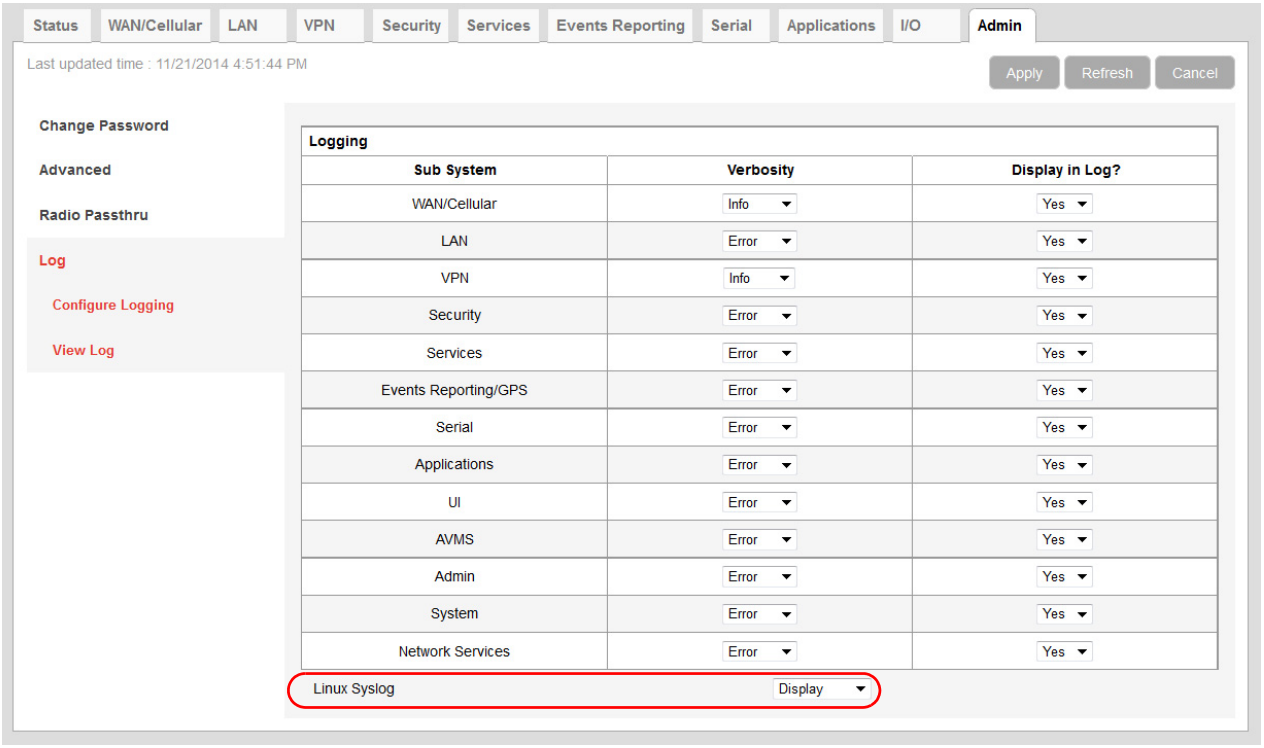
Check the format of the SMS command. There should be no space between the prefix and the command (or the 1st command parameter in the case of multi-parameter commands), and a single space between all other fields to act as a delimiter. For more information, see SMS Commands on page 328 and SMS Overview on page 149.

VPN

My VPN connection is not working. When I try to debug it using the logs on the Admin page, VPN information does not show up in the log.

VPN information is collected in the Linux logs. To view this information:

1. Log into ACEmanager as User and go to Admin > Log.



2. In the drop-down menu beside Linux Syslog, ensure that Display is selected.
   If you change the setting:
   a. Click Apply.
   b. Reboot the device.
3. Click View Log.
4. On the View Log page, click Clear and then click Refresh.

VPN Troubleshooting

If you see the following lines in the log, it means the VPN Server is not answering.

```
notice openvpn[9199]: [UNDEF] Inactivity timeout (--ping-restart), restarting
notice openvpn[9199]: TCP/UDP: Closing socket
```

Check the VPN Server status.

When I configure a VPN, my Internet connection stops working.

When you configure a VPN, outgoing traffic from the host to the public Internet is blocked by default, as a security measure. If you want to enable public Internet traffic from the host:

1. In ACEmanager, go to VPN > Split Tunnel.
2. Change the Outgoing Host Out of Band field to Allowed.
3. Click Apply.

Poor Wireless Network Connection

ACE manager indicates that my AirLink gateway has a poor wireless connection. What can I do to improve it?

For GSM or CDMA networks:

1. Check the RSSI value. If ACEmanager (Status screen) indicates a good RSSI value, go to step 2. If it indicates a poor RSSI value:
   - Check the antenna connection.
   - Make sure you have the correct antenna for the device.
   - You may be in an area with poor coverage. Check with your Mobile Network Operator, or if possible, try moving the AirLink gateway to a new location.
2. Check the Ec/Io value. If ACEmanager (Status screen) indicates a poor Ec/Io value:
   - This may be a temporary network problem caused by local interference.
   - A nearby laptop or other electronic equipment may be interfering with the signal. Try moving the AirLink gateway to a different location.

For LTE networks:

1. Check the RSSI value. If ACEmanager (Status screen) indicates a good RSSI value, go to step 2. If it indicates a poor RSSI value:
   - Check the antenna connection.
   - Make sure you have the correct antenna for the device.
   - Try moving the AirLink gateway to a different location.
2. Check the RSRP value. If ACEmanager (Status screen) indicates a good RSRP value, go to step 3. If it indicates a poor RSRP value:
   - This may be a temporary network problem caused by local interference.
   - Check the antenna connection.
   - Make sure you have the correct antenna for the device.
   - You may be in an area with poor coverage. Check with your Mobile Network Operator, or if possible, try moving the AirLink gateway to a new location.
3. Check the RSRQ value. If ACEmanager (Status screen) indicates a poor RSRQ value:

- A nearby laptop or other electronic equipment may be interfering with the signal. Try moving the AirLink gateway to a different location.

Connection not working

My device appears to be connected to the host, but no data is being transferred.

1. Check to see if MAC filtering is enabled (Security > MAC Filtering).
2. If MAC filtering is enabled:

- Ensure that the MAC Address for the host in question is on the Allowed List.
- Ensure that there are no typos in the MAC Address.

  Or

- If it is not required, disable MAC Filtering and reboot the device.

My host device is unable to connect to the Internet, even when there is good mobile network coverage and ALEOS can Ping an external IP address.

1. Check the DNS proxy setting described on page 97.

   You may need to change this setting to Disable so that all connected hosts acquire the Mobile Network Operator-defined DNS server as the first DNS server. The AirLink gateway is not used as the DNS resolver.

Updating the ALEOS Software and Radio Module Firmware

I am unable to update the ALEOS software and radio module firmware using ACEmanager.

If you are having trouble updating the ALEOS software or radio module firmware, especially if you are updating from an older version of ALEOS:

1. Try using a different browser. (ACEmanager supports the latest versions of Internet Explorer and Firefox.)
2. Delete the browser cookies/cache before logging into ACEmanager. (The Web browser short-cut is Control + Shift + Delete.)
3. Backup your device settings by downloading and saving the template. See Saving a Custom Configuration as a Template on page 14.
4. Reset the device to factory default settings. (See Reset to Factory Default on page 231 or press and hold the reset button on the device for 7 to 10 seconds.)
5. If you are updating from ALEOS 4.3.3 or earlier, be sure to follow the correct software update path. For more information, refer to the Upgrading to ALEOS 4.3.4 from Older Versions Application Note (part number 4115254) available on source.sierrawireless.com.
6. Begin the update process (see Update the ALEOS Software and Radio Module Firmware on page 18) and follow the prompts.

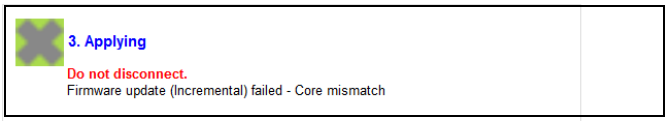
7. If after 30 minutes the Web UI is frozen, log in using a different browser and confirm whether or not the ALEOS software and radio module firmware has been updated correctly.
8. If you are still having problems, contact your Sierra Wireless distributor.

When I am trying to update the radio module firmware, the connection times out and I cannot reconnect to the device.

Depending on the file size and the connection speed, it can take 10 to 20 minutes to upload and install the radio module firmware. While this is taking place, you may see a "connection timed out" message. You can ignore this message, as the connection is still valid and the firmware update process is continuing. If you are connected to the device over-the-air, you will not be able to access the device until the radio module update is complete.

1. Continue to wait for the process to complete and the device to reboot.
   - **Do Not** reset the device.
   - **Do Not** disconnect the power.
   - **Do Not** click Cancel.
2. If after 20 minutes, the device does not reboot, contact Sierra Wireless Technical Support.

When I try to update ALEOS using ACEmanager, I see the following message: "Firmware update (Incremental) failed - Core mismatch".

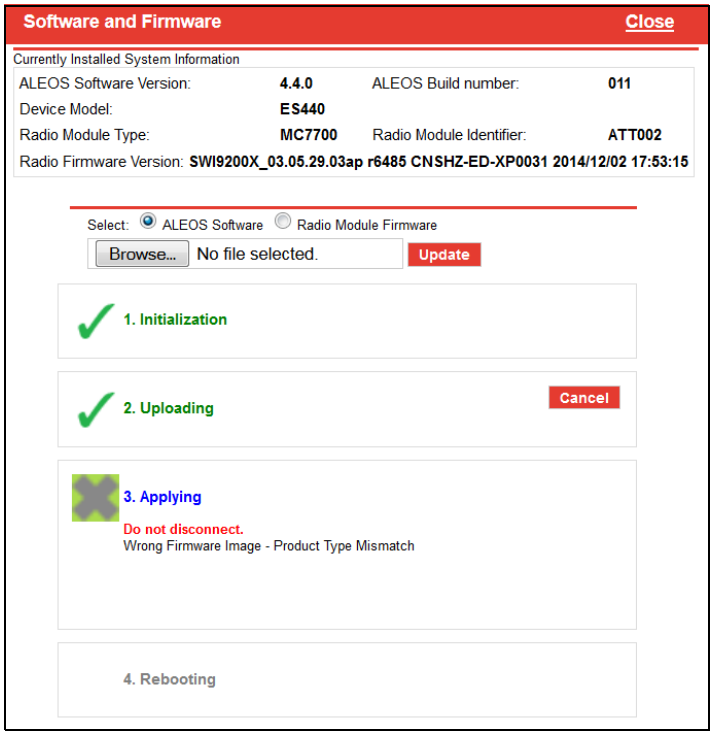


This message appears when the device you are trying to update the AirLink gateway with an Incremental ALEOS version.

To correct the problem:

1. Click Cancel.
2. Close ACEmanager.
3. Ensure that you have downloaded the correct ALEOS version for your device and Mobile Network Operator.
4. Re-launch ACEmanger, log in, click the Firmware link, and retry the Software and firmware update.

When I try to update ALEOS using ACEmanager, I see the following message: “Firmware update failed - Bad image”.

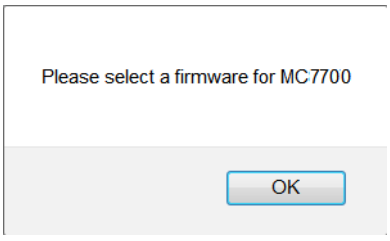


This message also appears if you are only updating the radio module firmware and you have the Update ALEOS radio button selected.

To correct the problem:

1. Close the Update page.
2. Retry the radio firmware update, being careful to select the Radio Module Firmware button before clicking Browse.

When I try to update ALEOS using ACEmanager, I see the following message: “Please select a firmware for xxxx”.



This message appears and you are blocked from continuing with the update if you are only updating the radio module and you select a radio module firmware file designed for a different radio module.

To correct the problem:

1. Click OK.

2. Select a radio module firmware file for the radio module in the AirLink gateway you are updating and click update. (To check which radio module is in your device, in ACEmanager, go to Status > About.)

AirVantage Management Service

I don't understand the message that appears in the Status field in the Services > AVMS page.

The error messages in the Services > AVMS > Status field can be due to a communication failure, a problem with the AVMS server, or a failure when parsing a valid AVMS server response. The following table describes the error messages and the corrective action.

Error message	Meaning	Corrective action
Communication Failure Errors		
[HTTP] Initialization error	The transfer object could not be initialized.	Contact AVMS support[a].
[HTTP] Unsupported protocol	The AVMS server URL protocol is not supported.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com.
[HTTP] Failed initialization	The transfer library could not be initialized.	Contact AVMS support[a].
[HTTP] URL using bad/illegal format or missing URL	The AVMS server URL is missing or not properly formatted.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com.
[HTTP] Couldn't resolve host name	The AVMS server URL could not be resolved.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com. Also check the cellular connectivity.
[HTTP] Couldn't connect to server	Connection to the AVMS server URL failed.	In ACEmanager, check the AVMS URL in the Service > AVMS > Server URL field. The default value is http://na.m2mop.net/device/msci/com. Also check the cellular connectivity.
[HTTP] Timeout was reached	The transfer timeout (equal to the communication period if defined or 5 minutes) expired.	Check cellular connectivity.
[HTTP] Server returned nothing (no headers, no data)	No data was received from the AVMS server.	Check cellular connectivity.
[HTTP] Unrecognized or bad HTTP Content or Transfer-Encoding	The AVMS server HTTP response contains a malformed content or transfer-encoding header field.	Contact AVMS support[a].
[HTTP] Out of memory	A memory allocation problem occurred.	Contact AVMS support[a].

Error message	Meaning	Corrective action
[HTTP] SSL peer certificate or SSH remote key was not OK	This message appears if you are using an HTTPS server URL, the SSL Verify Peer Certificate field is set to Enable, and the server SSL certificate validation fails. If this happens, communication with the AVMS server is terminated.	If you see this error message: 1. Check to see that you have a valid URL in the Server URL field. 2. In ACEmanager, go to Admin > Advanced and check the Date and Time field to confirm that the values are correct.[b] The SSL certificates have a start and end date. If the device has a date and time outside of this interval, the certification check will fail. 3. Contact your IT Administrator, or if you want the traffic to go through without verifying the server certificate, change the setting in the Services > AVMS > SSL Verify Peer Certificate field (described on page 140) to Disable.
AVMS Server Errors		
[AVMS] HTTP error '500'	AVMS server reported error 500 in the HTTP response.	Refer to the available AVMS server documentation for a list of all possible error codes and their significance.
Error message indicating a failure when parsing a valid AVMS server response		
XML processing error	The content of a valid AVMS server response cannot be parsed.	AVMS server responses are mal-formatted. Contact AVMS support[a].

a. AVMS technical support: https://issues.m2mop.net
b. If the values are not correct and the device is not receiving date and time from the Mobile Network Operator or GPS, go to Services > Time (SNTP), and enable time update. For the SNTP Server, use the same service as the authenticating server.

LTE Networks

How do I interpret the number shown in the Band Class field on the Status > WAN Cellular page for a device on an LTE network?

Use the following table to interpret the values in the LTE Band Class field in ACEmanager (STATUS > WAN Cellular).

Band Class number	Uplink frequency range (MHz)	Downlink frequency range (MHz)
120	1920–1980	2110–2170
121	1850–1910	1930–1990
122	1710–1785	1805–1880
123	1710–1755	2110–2155
124	824–849	869–894
125	830–840	875–885
126	2500–2570	2620–2690

Band Class number	Uplink frequency range (MHz)	Downlink frequency range (MHz)
127	880–915	925–960
128	1749.9–1784.9	1844.9–1879.9
129	1710–1770	2110–2170
130	1427.9–1452.9	1475.9–1500.9
131	698–716	728–746
132	777–787	746–756
133	788–798	758–768
134–135	Reserved for bands 15 and 16	
136	704–716	734–746
137	815–830	860–875
138	830–845	875–890
139	832–862	791–821
140	1447.9–1462.9	1495.9–1510.9
141–151	Reserved for bands 22 to 32	
152	1900–1920	1900–1920
153	2010–2025	2010–2025
154	1850–1910	1850–1910
155	1930–1990	1930–1990
156	1910–1930	1910–1930
157	2570–2620	2570–2620
158	1880–1920	1880–1920
159	2300–2400	2300–2400

How do I obtain and interpret SINR values for LTE networks?

You can use the AT*CELLINFO? command to obtain an SINR (Signal to Interference plus Noise Ratio) value. (See *CELLINFO2? on page 285.)

The values vary depending on the network characteristics and the AirLink gateway, but in general, a positive value provides usable throughput. The following table provides guidelines for interpreting SINR values.

SINR Value	Throughput
< 0	Poor
0 to 5	Fair

SINR Value	Throughput
6 to 10	Good
> 10	Excellent

If the SINR value indicates poor throughput:

- Move the antenna away from noisy equipment.
- Move closer to the nearest cell tower line of sight, or further away from the interfering cell tower.

SIM Card is Blocked

My SIM card has a PIN number. I've entered the wrong PIN several times and now the SIM card is blocked.

AirLink products do not support Personal Unlocking Key (PUK) entry. However, if you need to unblock the SIM card:

1. Contact your Mobile Network Operator to obtain the PUK.
2. Remove the SIM card from the AirLink gateway and insert it in a cell phone that accommodates a MiniSIM (2FF) card.
3. Enter the PUK to unblock the SIM card and then return the SIM card to the AirLink gateway.

Note: Be careful when entering the PUK. You have a limited number of attempts to enter the correct PUK (generally 10) before the SIM card is permanently disabled and a new SIM card is required. If the PUK does not unblock the SIM card after the first few attempts, contact your Mobile Network Operator.

Remote connections

I cannot connect to the AirLink gateway remotely over the Mobile Network Operator's Private Network via the Web UI, although I can connect to it locally.

Some Mobile Network Operators' private networks have restrictions on the maximum transmission unit (MTU) size. This is more prevalent with LTE networks.

Possible solutions:

- Use your Mobile Network Operator's public network.
- Ask your Mobile Network Operator to reduce the MTU size on the router or other equipment at their end of the private network. Setting the MTU value below 1500 bytes (for example 1326 bytes) has resolved the problem on some private networks.
- If your AirLink gateway has a radio module (such as the MC7700 or MC7750) that supports LTE networks, select an option in ACEmanager (WAN/Cellular > Advanced > Setting for Band field) that excludes LTE networks.

Radio Band Selection

I set the radio band in the UI (WAN/Cellular > Setting the Band) or by using the AT!BAND AT command, but after I reboot the band setting reverts to its former value.

For some SIM cards, you need to set the band before inserting the SIM card.

To resolve this problem:

1. Remove the SIM card.
2. Set the band to the desired value.
3. Reboot the device.
4. Insert the SIM card.

Reliable Static Routing (RSR)

I launched ACEmanager with Internet Explorer 9. I configured RSR, but after I enabled RSR and clicked Apply, all the values reverted to the defaults.

There is a known issue. If you configure and enable RSR with ACEmanager in Internet Explorer 9, and then click Apply, the values in the ACEmanager screen appear as default values.

This is an ACEmanager display issue only. The configuration is applied properly, but the configured values are not displayed. Click Refresh to view the configured values.

Inbound Ports Used by ALEOS

When I configure ports for an application on a LAN client such as a router or laptop, I want to ensure that the ports I use do not conflict with the inbound ports that ALEOS uses. Which ports does ALEOS use?

Table E-1 shows the inbound ports that are set in ALEOS and cannot be configured. Table E-2 show the default setting for ports you can configure and where to change the ports in ACEmanager.

Table E-1: ALEOS Non-configurable Inbound Ports

Port	Use
9494 – 9497 17335 17345 – 17353 21000 – 21003	Used internally for GPS and Events Reports
500 4500	Used internally for IPSec VPN
8088	Used internally for AVMS

Table E-2: ALEOS Configurable Inbound Ports

Default Port	Feature	ACEmanager location
161	SNMP Port	Services > Management (SNMP)
2332	SSH/Telnet Remote Login Server Port	Services > Telnet/SSH
9191	ACEmanager Port	Services > ACEmanager
9300	SSL tunnel Port	VPN > SSL Tunnel
9443	ACEmanager SSL Port	Services > ACEmanager
9494	GPS Poll Port	GPS > Global Settings
12345	Device Port used for incoming TCP/ UDP traffic	Serial > Port Configuration

Event Reporting

I set up ACEmanager to send an email/SMS report, but when I clicked the Test report button no report was sent.

After you set up the event reporting fields and click Apply, wait about a minute before you click the Test report button. The AirLink gateway needs this time to apply the new configuration.

I configured event reporting, but I did not receive a report when I should have.

- If the Action Type for the Event Reporting is Email or SNMP TRAP, be sure that these services are also configured on the Services tab.
  - To configure email, go to Services > Email (SMTP).
  - To configure SNMP TRAP, go the Services > Management (SNMP).

TCP/IP and UDP/IP Auto Answer

I configured TCP/UDP auto answer, but the packet contents are not being streamed over the serial port to the connected device.

1. Try polling the device connected to the AirLink gateway's serial port.

   If you do not receive a response, confirm that the fields described in Configuring IP to Serial with Auto Answer and Serial to IP on page 207 are set correctly.
2. In ACEmanager, go to Status > Serial and check the Serial bytes sent field to confirm that packets are reaching the AirLink gateway from the mobile network and the packet contents are being sent out the AirLink gateway's serial port.

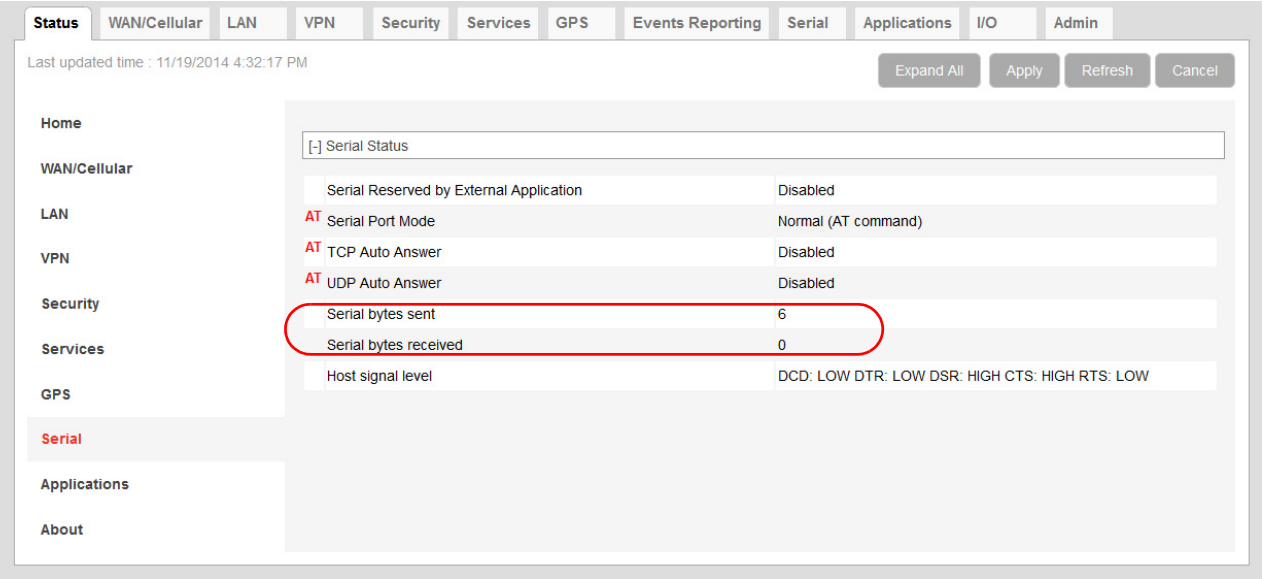


Figure 5-1: ACEmanager: Status > Serial

When you poll the AirLink gateway/connected device:

- If the Serial bytes sent counter increases, the IP packets have reached the AirLink gateway from the mobile network, the AirLink gateway has removed the header and sent the packet contents out its serial port to the connected device.
- If the Serial bytes sent counter does not increase, either:
  - The IP packet has not made it across the mobile network to the AirLink gateway.
  - The destination port for the TCP/IP or UDP/IP connection does not match the configured Device Port on the ACEmanager Serial tab.

3. Once you have confirmed that the Serial bytes sent counter is increasing, check the Serial bytes received counter (also on the Status > Serial screen).
   - If the Serial bytes received counter is increasing, the connected device is responding to the poll request and sending its response back to the AirLink gateway across the serial connection.
   - If the Serial bytes received counter is not increasing, the connected device is not responding to the poll request. Ensure that the serial cable is fully seated and properly connected to the AirLink gateway and the host. Check that you have the correct type of serial cable connecting the AirLink gateway to the connected device. The AirLink gateway is a DCE device. If the connected device is also a DCE device, use a null modem serial cable. If the connected device is a DTE device, use a straight through serial cable.
4. If you have confirmed that both the Serial bytes sent and Serial bytes received counters are increasing when you send a poll to the connected device, but you are still not receiving the response back on your original sending application, the most common reason is that the incoming packets from the AirLink gateway to your application are being blocked by a firewall on your network. The firewall may be blocking all traffic except packets destined for particular ports or arriving from particular ports.

   Check with your firewall administrator. Ask the administrator to monitor the firewall when you poll the AirLink/connected device to see if any return packets from the AirLink gateway hit the firewall.

If you are still having problems, contact your Sierra Wireless distributor.

Templates

The template does not upload properly when I use Internet Explorer 9.

To resolve the problem:

1. In Internet Explorer 9, go to Tools > Internet Options.
2. Select the Security tab.

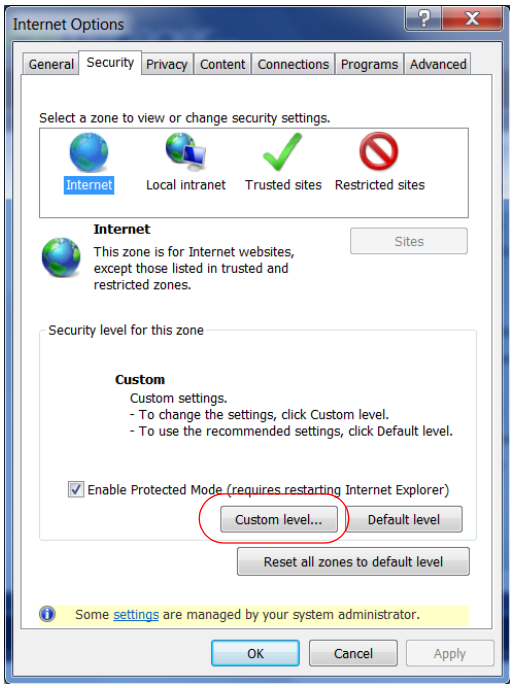


Figure 5-2: Internet Explorer 9: Tools > Internet Options > Security tab

3. Click Custom level....
4. Scroll down until you see “Include local directory path when uploading files to a server”.
5. Select Disable.

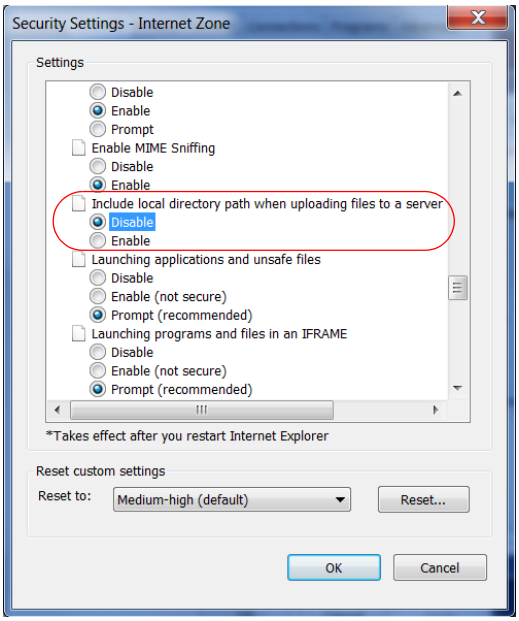


Figure E-3: Internet Explorer 9: Security Settings

6. Click OK.

F: Glossary of Terms

Acronym or Term	Definition
1xEV-DO	Single Carrier (1X) EVolution–Data Only A high-speed standard for cellular packet data communications. It supports Internet connections with data rates up to 3.1 Mbps. (downlink from the network) and 1.8 Mbps (uplink to the network). Average data rates are approximately: • Rev. A: 600-1300 kbps. (downlink from the network) and 300-400 kbps (uplink to the network) • Rev. 0: 400-700 kbps (downlink from the network) and 40-80 kbps (uplink to the network) Actual speed depends on the network conditions. Compare to 1X.
1X	Single Carrier (1X) Radio Transmission Technology A high-speed standard for cellular packet data communications. 1x supports Internet connections with data rates up to 153 kbps (simultaneously in each direction—downlink and uplink). Actual speed depends on the network conditions. Compare to 1xEV-DO.
3GPP	3rd Generation Partnership Project 3GPP unites 6 telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TTA, TTC), and provides their members with a stable environment to produce Reports and Specifications that define 3GPP technologies.
API	Programming Interface A protocol intended to be used as an interface by software components to communicate with each other.
AT	A set of device commands, preceded by “AT” originally developed by Hayes, Inc. for their devices. The structure (but not the specific commands, which vary greatly from manufacturer to manufacturer) is a de facto device industry standard.
CDG	CDMA Development Group A consortium of companies who joined together to lead the adoption and evolution of CDMA wireless systems around the world. Also see CDMA.
CDMA	Code Division Multiple Access A wideband spread spectrum technique used in digital cellular, personal communications services, and other wireless networks. Wide channels (1.25 MHz) are obtained through spread spectrum transmissions, thus allowing many active users to share the same channel. Each user is assigned a unique digital code, which differentiates the individual conversations on the same channel.
cdmaOne	A IS-95 CDMA standard developed by QUALCOMM Inc. Also known as TIA-EIA-95.
CE, CE Label	The CE label is a mandatory conformity marking for products placed on the market in the European Economic Area (EEA). With the CE marking on a product, the manufacturer declares that the product conforms with the essential requirements of the applicable EC directives.

Acronym or Term	Definition
CnS	Sierra Wireless' proprietary Control and Status protocol interface
DCE	Data Communications Equipment A device that sits between the data terminal equipment (DTE) and a data transmission circuit. Usually the DCE is a modem.
DMNR	Dynamic Mobile Network Routing
Diversity	Antenna diversity, also called space diversity, is a scheme that uses two or more antennas to improve the quality and reliability of a wireless link. Often, especially in urban and indoor environments, there is no clear line-of-sight (LOS) between transmitter and receiver. Instead the signal is reflected along multiple paths before finally being received. Each bounce can introduce phase shifts, time delays, attenuations, and distortions that can destructively interfere with one another at the aperture of the receiving antenna.
EDGE	Enhanced Data rates for GSM Evolution A digital mobile phone technology that allows improved data transmission rates as a backward-compatible extension of GSM. EDGE is considered a pre-3G radio technology and is part of ITU's 3G definition. Also known as Enhanced GPRS (EGPRS), or IMT Single Carrier (IMT-SC), or Enhanced Data rates for Global Evolution.
EIA	Electronics Industry Association EIA was a standards and trade organization composed as an alliance of trade associations for electronics manufacturers in the United States. They developed standards to ensure the equipment of different manufacturers was compatible and interchangeable. The EIA ceased operations on February 11, 2011, but the former sectors continue to serve the constituencies of EIA.
EMC	Electromagnetic Compatibility The branch of electrical science which studies the unintentional generation, propagation and reception of electromagnetic energy with reference to the unwanted effects (Electromagnetic interference, or EMI) that such energy may induce.
EMI	Electromagnetic Interference The disturbance that affects an electrical circuit due to either electromagnetic induction or electromagnetic radiation emitted from an external source
ERP	Effective Radiated Power A standardized theoretical measurement of radio frequency (RF) energy. It is determined by subtracting system losses and adding system gains.
ESN	Electronic Serial Number The unique first-generation serial number assigned to the Air Link devices for use on the wireless network. Compare to MEID.
Ethernet	Computer networking technologies for local area networks (LANs).
EU	The European Union Organization of European countries.

Acronym or Term	Definition
EVDO	Enhanced Voice-Data Optimized or Enhanced Voice-Data Only (Ev-DO, EV, EVDO, etc.). A telecommunications standard for the wireless transmission of data through radio signals, typically for broadband Internet access. It uses multiplexing techniques including code division multiple access (CDMA) as well as time division multiplexing (TDM) to maximize both individual users' throughput and the overall system throughput.
FCC	Federal Communications Commission The U.S. federal agency responsible for interstate and foreign communications. The FCC regulates commercial and private radio spectrum management, sets rates for communications services, determines standards for equipment, and controls broadcast licensing.
FW	Firmware Software stored in ROM or EEPROM; essential programs that remains even when the system is turned off. Firmware is easier to change than hardware but more permanent than software stored on disk.
GPRS	General Packet Radio Service A packet-oriented mobile data service on 2G and 3G cellular communication systems. GPRS was originally standardized by European Telecommunications Standards Institute (ETSI) in response to the earlier CDPD and i-mode packet-switched cellular technologies. It is now maintained by the 3rd Generation Partnership Project (3GPP).
GSM	Global System for Mobile Communications (originally Groupe Spécial Mobile) GSM is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital mobile networks used by mobile phones
HSPA	High Speed Packet Access An amalgamation of two mobile telephony protocols: High Speed Downlink Packet Access (HSDPA) and High Speed Uplink Packet Access (HSUPA). This extends and improves the performance of existing 3rd generation mobile telecommunication networks utilizing the WCDMA protocols.
HSPA+	Also called evolved HSPA This allows bit-rates to reach as high as 168 Mbit/s in the downlink and 22 Mbit/s in the uplink. An improved 3GPP standard.
IC	Industry Canada The government department responsible for overseeing and regulating wireless and communication technologies in Canada.
IEC	International Electrotechnical Commission A non-governmental international standards organization that prepares and publishes International Standards for all electrical, electronic and related technologies – collectively known as “electro technology.”
IOTA	Internet Over The Air An automated feature, supported by some service providers, to perform account setup by making a connection to the CDMA network and using a secure Internet connection to download account parameters to the device.

Acronym or Term	Definition
IS	Interim Standard After receiving industry consensus, the TIA/EIA forwards the standard to ANSI for approval.
IS-95	A 2G mobile telecommunications standard using CDMA to send voice, data and signaling data (such as a dialed telephone number) between mobile telephones and cell sites.
ISAKMP	Internet Security Association and Key Management Protocol A security protocol defined by RFC 2408 for establishing Security Associations (SA) and cryptographic keys in an Internet environment. ISAKMP only provides a framework for authentication and key exchange and is designed to be key exchange independent.
ITU	International Telecommunication Union A specialized agency of the United Nations responsible for issues that concern information and communication technologies. The ITU coordinates the shared global use of the radio spectrum, promotes international cooperation in assigning satellite orbits, and assists in the development and coordination of worldwide technical standards.
kbps	Kilobits per second 1000, not 1024, as used in computer memory size measurements of kilobytes.
LED	Light Emitting Diode A semiconductor diode that emits visible or infrared light.
LTE	Long Term Evolution High performance air interface for cellular mobile communication systems.
Mbps	Millions of bits per second, or Megabits per second.
MEID	Mobile Equipment IDentifier The unique second-generation serial n umber assigned to the device for use on the wireless network. *Compare to* ESN.
MSCI	Modem Status Configuration Interface ALEOS internal configuration database
NAM	Number Assignment Module Semi-permanent information stored in the device's non-volatile memory, including the device's Mobile Identification Number, the station class mark, Mobile Network Operator code, and other cellular identifiers. Essentially the phone number, it should be treated as confidential information and should not be disclosed to anyone other than the cellular service provider.
NV	Non-Volatile (memory)
OEM	Original Equipment Manufacturer A company that manufactures a product and sells it to a reseller.
OTAPA	Over the Air Parameter Administration A way of distributing new software updates or configuration settings to devices like cellphones and set-top boxes.
OTASP	Over the Air Service Provisioning. Also see OTAPA.

Acronym or Term	Definition
PAD	Packet Assembly/Disassembly
PCS	Personal Communications Services A cellular communication infrastructure that uses a different frequency range than AMPS.
PPP	Point to Point Protocol An alternative communications protocol used between computers, or between computers and routers on the Internet. PPP is an enhanced SLIP. Also see SLIP.
PRI	Product Release Instructions A file containing the settings used to configure devices for a particular service provider, customer, or purpose.
RF	Radio Frequency
RoHS	Restriction of use of Hazardous Substances mandated by EU Directive 2002/95.
RS-232	A series of standards for serial binary single-ended data and control signals connecting between a DTE (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports.
Rx	Receive
SIM, SIM Card	Subscriber identity module or subscriber identification module. An integrated circuit which securely stores the international mobile subscriber identity (IMSI) and the related key used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers).
SINR	Signal to Interference plus Noise Ratio (SINR) is an RF parameter that is directly proportional to throughput (the higher the number, the higher the throughput). It can help LTE radio installers gauge the signal quality between the cell tower and the radio module. For more information on interpreting the SINR values, see How do I obtain and interpret SINR values for LTE networks? on page 340.
SKU	Stock Keeping Unit Identifies an inventory item: a unique code, consisting of numbers or letters and numbers, assigned to a product by a retailer for purposes of identification and inventory control.
SLIP	Serial Line Internet (or Interface) Protocol An Internet Protocol designed to work over serial ports and modem connections. On personal computers, SLIP has been largely replaced by the Point-to-Point Protocol (PPP), which has more features and does not require its IP address configuration to be set before it is established. On microcontrollers SLIP is still the preferred way of encapsulating IP packets due to its very small overhead. Also see PPP.
SMS	Short Message Service A feature which allows users of a wireless device on a wireless network to receive or transmit short electronic alphanumeric messages (up to 160 characters, depending on the service provider).
TCH	Traffic Channel

Acronym or Term	Definition
TIA/EIA	Telecommunications Industry Association / Electronics Industry Association A standards setting trade organization, whose members provide communications and information technology products, systems, distribution services and professional services in the United States and around the world.
Tx	Transmit
UMTS	Universal Mobile Telecommunications System (UMTS). A third generation mobile cellular system for networks based on the GSM standard. Developed and maintained by the 3GPP (3rd Generation Partnership Project), UMTS is a component of the International Telecommunications Union IMT-2000 standard set and compares with the CDMA2000 standard set for networks based on the competing cdmaOne technology.
USB	Universal Serial Bus An industry standard defining the cables, connectors and communications protocols used in a bus for connection, communication and power supply between computers and electronic devices.
VRRP	Virtual Router Redundancy Protocol
X.509	A Public Key Infrastructure (PKI) and Privilege Management Infrastructure (PMI) are standards that specify formats for public key certificates, certificate revocation lists, attribute certificates, a certification path validation algorithm, etc.

Index

A

ACEmanager, 140
  configuring, 13
  description, 10
  idle timeout, set, 141
  login, 12
  overview, 10
ALEOS Application Framework
  troubleshooting, 332
  unable to load application from, 332
  using, 217, 225
ALEOS software update, 18
always on connect, 57, 161
analog inputs
  channel configuration, 286
APN
  backup, 64
applications, 212
  status, 48
AT Commands
  Applications > Data Usage, 324, 325
  I/O > Current State, 324
  Security > Trusted IPs - Inbound, 299, 304
  Serial > Port Configuration, 313
  Services > Low Power, 305
  Status > Home, 284, 318
authentication
  general information, 178
  LDAP, 178
  RADIUS, 180
  TACACS+, 181
Auto DHCP, 88
AVMS
  auto synchronize, 139
  configuration, 138

B

Bands, LTE, 339
bandwidth throttle, 65
browser support, 12

C

configuration
  application, 212
  LAN, 79
  logging, 234
  serial, 193
  services, 138
  VPN, 110
connection not working, 335
custom SSL certificate, 141

D

data usage, 212
Dead Peer Detection, 116
device status (about), 49
Device Status Screen
  configuring, 183
DHCP Options, 83
DHCP/Addressing, 80
Dial-up Networking, 237
digital inputs
  uses, 220
DMNR, 72
DMZ, 131
DNS
  alternate port, 97
  dynamic, 142
  global, 96
  override, 97
DNS proxy
  configure, 97
documentation, 10, 11
domain name, 147
DUN
  operating systems supported, 237
  setting up, 237
Dynamic Mobile Network Routing *See* DMNR

E

EC/IO, 32
email
  SMTP, 169
  test, 166
Ethernet
  status, 40
Ethernet ports, 87
  troubleshooting, 331
Extended Archiver, 231

F

firmware update, 18

G

global DNS, 96
Glossary, 347
GRE, 118

H

Host Interface Watchdog, 108
host port routing, 26, 94

I

Idle timeout, ACEmanager, 141
inbound ports used by ALEOS, 342
Internal DHCP Server, 86
IP Logging, 229
IP Manager, 145
IPsec, 111

IPv6
cellular address (LTE, fallback to EV-DO), 35
configuring support for, 53
prefix length (LTE, fallback to EV-DO), 36

K

keepalive, 60

L

LAN
configuration, 79
management, 26
status, 39
LDAP authentication, 178
LED indicator for serial traffic, 193
LEDs, above Ethernet port, 331
Load Root Certificate, 122
Log, mark a section of the log, 233
logging
configuration, 234
Extended Archiver, 231
IP logging, 229
login, 12
LTE Band Class field, 339

M

MAC filtering, 136, 335
MIB (Management Information Base), 257

N

network connection, poor, 334
network settings, retain over reset, 232
Network State, 31
Network Watchdog, disable, 54, 55

O

Over the Air (OTA) connections, 26

P

password, change, 224
PCI compliance, 27
ping, on demand, 228
port filtering
inbound, 132
outbound, 133
port forwarding, 126
error message, 331
troubleshooting, 331
PPP connection, configuring, 205
PPPoE, 97
public and private mode, 79
pulse count, 222

R

radio band, selecting, 342
radio module firmware update, 18
radio passthru, 233
RADIUS authentication, 180
re-activation, 64
relay outputs, 221
Reliable Static Routing (RSR), 68
reset device, retain network settings, 232
reset, periodic and time of day, 227
reverse telnet/SSH, 196
RSCP, 32
RSRP, 33
RSRQ, 33
RSSI, 32

S

security
configuration, 126
status, 44
serial
configuration, 193
LED indicator, 211
MTU, 195
status, 46
serial port
port configuration, 194
PPP, 206
TCP, 202
UDP, 203
services
configuration, 138
status, 45
Simple Network Management Protocol (SNMP), 172
SINR, 340
SLIP, 205
SMS, 149
advanced, 165
Control Only mode, 152
Gateway Only mode, 153
M2M, 166
Password, 163
Password Only mode, 151
password, default, 164
Quick Test, 166
security, 162
test, 166
troubleshooting, 332
trusted phone number, 163
SMS Commands, 328
SMS M2M, 166
SMS message error, 332
SMS Wakeup, 160
SNMP traps, 257
SNTP, 177
split tunnel, 110
SSH, 168
SSL tunnel, 119

Status
About, 49
Applications, 48
Home, 29
LAN, 39
Security, 44
Serial, 46
Services, 45
VPN, 42
WAN/Cellular, 35

T

TACACS+ authentication, 181
TCP connection
configuring, 201
Telnet, 168
template
applying, 16
saving a custom configuration as, 14
test button, SMS/email, 166
third party services, 144
time (SNTP), 177
troubleshooting
AAF, 332
AVMS status messages, 338
Ethernet ports, 331
LAN network, 331
mark a section of the log, 233
port forwarding, 331
radio module firmware update, 335
RSR, 342
SMS, 332
software and radio firmware updates, 335
VPN, 333
wireless connection, 334, 335
trusted IPs
inbound, 134
outbound, 136
Trusted Phone Number, 163

U

UDP connection
configuring, 203
update
ALEOS software, 18
radio module firmware, 18
USB drivers, installing, 92
USB port, 90

V

VLAN, 103
VPN
configuration, 110
Failover, 123
GRE, 118
IPsec, 111
SSL tunnel, 119
status, 42
troubleshooting, 333
VRRP, 104