AirLink Networking Solutions

Secure Deployment and Operation Guide

41112693
Rev 2

SIERRA WIRELESS®

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.

Do not operate the Sierra Wireless product in any aircraft, whether the aircraft is on the ground or in flight. In aircraft, the Sierra Wireless product **MUST BE POWERED OFF**. When operating, the Sierra Wireless product can transmit signals that could interfere with various onboard systems.

Note: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open. Sierra Wireless products may be used at this time.

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.

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

© 2023 Sierra Wireless. All rights reserved.

Trademarks

Sierra Wireless®, AirPrime®, 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

Revision History

Revision number	Release date	Changes
1	Sept. 30, 2019	New document
2	May 2023	Added ALMS recommendations to chapter 3

Contents

1: Security Overview

As the Internet of Things (IoT) becomes more prevalent, so do concerns over data security. Cyber attacks of all type—brute-force attacks, distributed denial of service attacks (DDoS), among others—can be launched any time, anywhere. While Sierra Wireless AirLink routers and gateways have many security features enabled “out of the box”, just by being deployed and online, they can be subject to these types of attacks. You must be vigilant and pro-active to truly secure your devices during their operational lifetime.

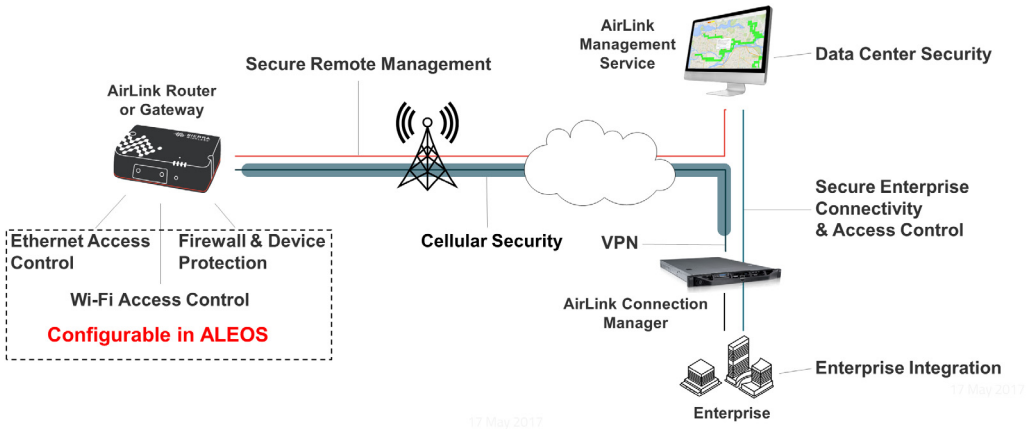
This guide has been created with the aim of giving you, as a system installer or administrator, IT support, or IT security employee, the information you need to deploy Sierra Wireless AirLink devices as part of a secure system. This guide will cover the following topics from the standpoint of optimizing security:

- **Installation**—device location, orientation, etc.
- **Configuration**—account management, firewalls, DMZ, and what features to enable or disable to minimize vulnerability
- **Services**—how to secure remote access to your devices, update firmware, as well as monitor devices for signs of attack
- **Appliances**—ensuring that AirLink Connection Manager provides security for connected devices and applications

Note: This guide covers aspects of security for Sierra Wireless products and services. Security is a responsibility shared between equipment/service providers (such as Sierra Wireless), system integrators (the people who plan and build the system) and end users (the people who configure and maintain the system). A well-coordinated and executed security strategy such as that outlined in this document will help ensure that customers have a consistent, successful experience.

System Overview

In every AirLink router or gateway deployment, there are various points in the system to which you should pay particular attention when it comes to security.



ALEOS, the embedded software on AirLink routers and gateways, is configured using ACEmanager (a web-based configuration utility). Security measures to employ in ALEOS are covered in Chapter 2.

AirLink Management Service (ALMS) and AM are services that give you control over device configuration and software updates, making it easier for your enterprise to provide devices with security updates, bug fixes and new security measures. See Chapter 3.

AirLink Connection Manager is a mobile-optimized VPN solution that consolidates security onto a single platform for all connected devices and applications in the vehicle area network. See Chapter 4.

Defense in Depth Strategy

An effective security strategy encompasses the following elements:

- ❑ Using a security appliance to limit access
- ❑ Managing system authentication with ALMS
- ❑ Strengthening authentication with a centralized authentication server (such as a RADIUS server)
- ❑ Detection—Monitor using ALMS and a SIEM (security information and event management) integration solution
- ❑ Remediation—Using a management system like ALMS for firmware updates and configuration changes

The following chapters describe how to apply these elements to Sierra Wireless AirLink products and services.

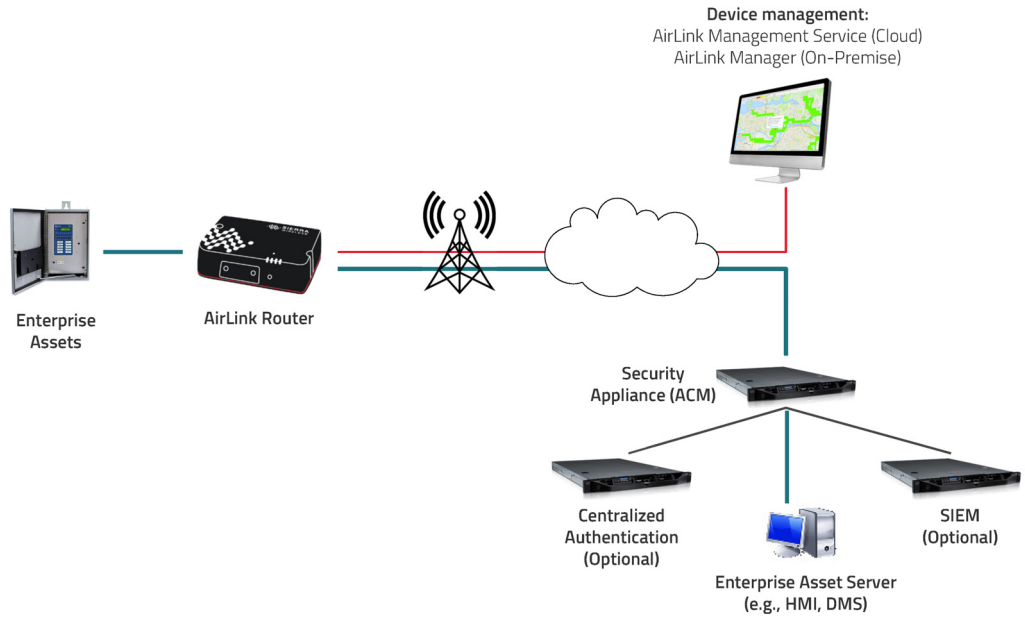


Figure 1-1: Recommended system architecture

2: Device Security

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 is a web application integrated in the ALEOS software that provides comprehensive configuration, monitoring, and control functionality to all AirLink gateways and routers.

ACEmanager can be accessed by:

- a local connection, via:
  - http by default on port 9191 (configurable)
  - https by default on port 9443 (configurable)
- a WAN-side (remote) connection if desired. Remote connection is disabled by default, but is configurable.

This chapter also covers the hardware aspects of security—best practices to follow when installing and maintaining the AirLink router or gateway.

Secure Installation

Each AirLink gateway or router has a Hardware User Guide that is available on the Source. These guides describe external product features and how to install the device. Following the installation procedures is an essential first step in securing your AirLink router or gateway.

Mounting the device with the recommended hardware (screws and/or mounting straps) helps ensure that the device cannot be easily stolen or tampered with.

In addition to the installation procedures, you should also ensure that the installation environment is safe from intrusion by unauthorized personnel. Ensure that utility rooms are secure and that routers or gateways installed in vehicles are inaccessible to passengers. Remember that the security of your vehicle fleet includes the security of your routers or gateways.

An AirLink router or gateway typically features the external features shown in Figure 2-1. While ensuring that your devices are secure, you must also be able to access these external features at times in order to read LEDs, manually reset devices, connect or reconnect ports. You must balance this practical consideration with the need for device security.

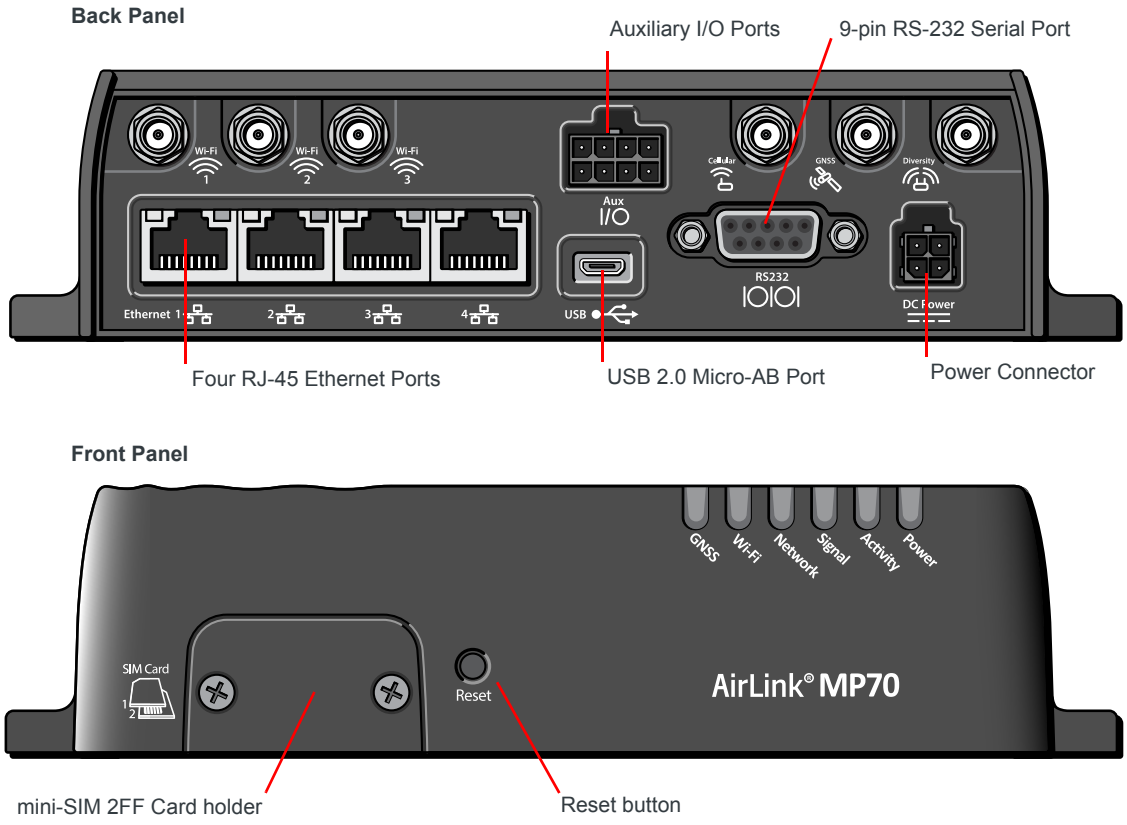


Figure 2-1: Connectors, LEDs and SIM Card Holder

Note: The AirLink MP70 router is shown in Figure 2-1. Not every AirLink router or gateway features the same number and type of ports. All AirLink products do feature a SIM card holder and reset button.

Because ACEmanager can be accessed by the USB, Ethernet and Serial ports, it is essential to secure those ports from unauthorized access.

You can disable or otherwise configure:
- Ethernet ports on the LAN > Ethernet page.
- USB on the LAN > USB page.
- Serial under Serial > RS232 Configuration

Defense in Depth Device Strategy

An effective security strategy encompasses the following elements:

❑ Disabling unused ports and services

For ACEmanager, this means:
- disabling unused USB, Serial, Ethernet and Wi-Fi ports and interfaces[1]

1. USB, Serial, and Ethernet ports are enabled by default on most AirLink routers and gateways.

- turning off ACEmanager remote access, Reverse Telnet, PAD auto-answer, port forwarding, DMZ, etc.

❑ Limiting access to enabled services

For ACEmanager, this includes using Trusted IP, PPPOE, MAC filtering, WPA/WPA2, VPN, Firewall rules

❑ Managing and Strengthening Authentication

This includes changing the default passwords, implementing password rotation with ALMS and a centralized authentication server.

Note: For a full discussion of recommendations for network authentication, see NIST Special Publication 800-63B, available at pages.nist.gov/800-63-3/sp800-63b

❑ Detection—SIEM with remote system, if applicable/suitable for your deployment. A SIEM solution can be expensive (given the data costs), but useful when investigating security events.

Checklist

Use the checklists in Table 2-1 and Table 2-2 to record which ports, interfaces, and services you intend to deploy, or have deployed, in your system.

Table 2-1: Ports and Interfaces

Port/Interface	Setting	Used	Unused
USB	LAN > USB > USB Device Mode	❑	❑
Serial	Serial > RS232 Port	❑	❑
Ethernet	LAN > Ethernet > Ethernet Port Configuration	❑	❑
Wi-Fi	Wi-Fi > General > Wi-Fi Modes	❑	❑

Table 2-2: Services

Service	Setting	Used	Unused
ACEmanager remote access	Services > ACEmanager > Remote Access	❑	❑
Reverse Telnet	Serial > Reverse Telnet > Autologin Reverse Telnet	❑	❑
PAD auto-answer	Serial > PAD > TCP Auto Answer	❑	❑
	Serial > PAD > UDP Auto Answer	❑	❑
Port forwarding	Security > Port Forwarding > Port Forwarding	❑	❑
DMZ	Security > Port Forwarding > DMZ Host Enabled	❑	❑
SNMP	Services > Management (SNMP) > SNMP Agent	❑	❑

Managing and Strengthening Authentication

More intrusions are caused by systems using default passwords than any other factor. Changing default passwords for AirLink routers and gateways after initially logging in is an essential early step in securing your device.

ALEOS devices have several passwords that should be changed from default whether they are going to be used or not, and recorded for future use.

Account Type	Description	ACEmanager setting
User	Administrator login for ACEmanager access	Admin > Change Password
AAF User	Login for installing AAF applications onto the gateway or router.	Admin > Change Password
Viewer	View-only ACEmanager access (removed from ALEOS 4.9.0 and later)	Admin > Change Password
M3DA	Used for managing AAF communications and access	Services > ALMS > AAF

For all devices, change the default user password, and consider using a unique password per device.

AirLink LX60, LX40, GX450, ES450, RV50, RV50X, RV55, and MP70 routers and gateways ship with a unique default password printed on the device label. Use this password as the user and M3DA password, and ensure that you change these passwords as soon as possible.

Note: When resetting the AirLink device to factory default settings, passwords will be reset to default if the Reset Mode is set to Reset All, or when you use the device's Reset button to reset the device to factory defaults.

Custom Certificate

For maximum security, you can select to use custom certificates to support the most secure https access.

The certificate must be an X.509 certificate; the private key must be in .pem format. They must be in separate files.

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.

You can upload custom certificates on the Services > ACEmanager page, under Advanced.

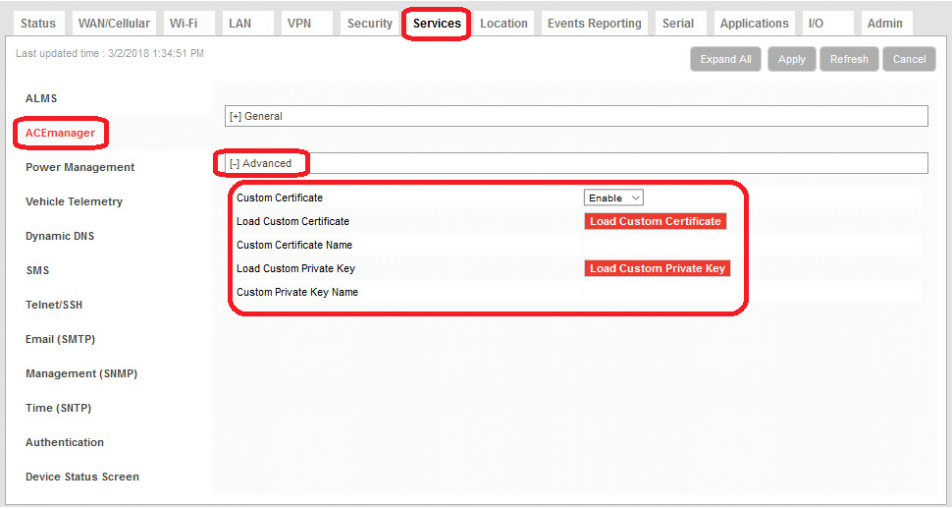


Figure 2-2: ACEmanager: Services > ACEmanager > Advanced

Limiting access to enabled services

Remote access to ACEmanager

As of ALEOS 4.9.0, remote access to ACEmanager over the WAN link is disabled by default.

If you want to enable remote access on a public network, you can enhance security by:

- setting access to HTTPS Only so that login traffic is encrypted
- specifying a non-default port for https access (default is 9443)

In summary, if you enable remote access on a public network, you should configure https-only access and consider changing the port from 9443.

Ensure that you document the changes for your Support providers.

To configure ACEmanager remote access, go to Services > ACEmanager.

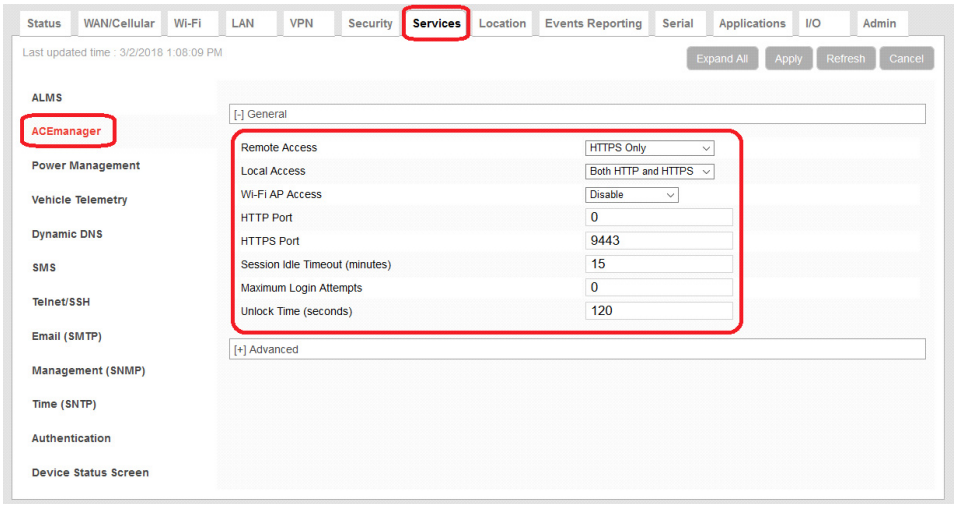


Figure 2-3: ACEmanager: Services > ACEmanager > General

Having remote access to ACEmanager can be useful for troubleshooting issues as long as the device is able to connect to the cellular network. Consider the following items in making your decision:

- Public or Private Cellular network—using a private cellular APN gives a significant level of security
- Allow only https:// access, which is recommended even on private networks, and very strongly recommended on public networks (when you should configure https or no ACEmanager access)
- Enable Maximum Login Attempts lock-out (if set to 0 [disabled]) and set the Unlock Time
- Configure inbound Trusted IP addresses for access (on the Security tab)

Firewall

Locking down devices exposed to public networks is essential for protection from security threats. You can configure port forwarding for your AirLink routers and gateways to allow traffic outbound, but not inbound.

These settings are available in ACEmanager on the Security tab.

DMZ Mode

By default, AirLink routers and gateways do not respond to unsolicited inbound traffic. DMZ Mode is disabled by default. Setting the DMZ mode to Automatic or Manual allows you to forward unsolicited inbound traffic to a specific device.

Automatic mode uses the first connected device. Select Manual and enter the IP address of the desired 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.

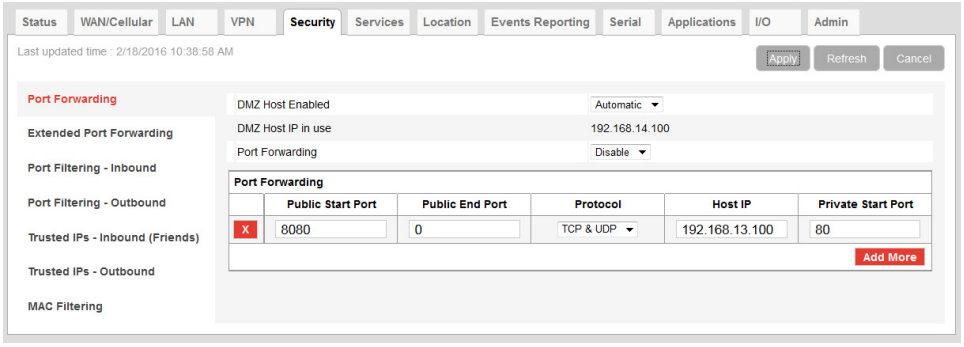


Figure 2-4: ACEmanager: Security > Port Forwarding (DMZ)

Port Forwarding and Filtering

If DMZ in Automatic mode is insufficient, you can configure specific Port Forwarding rules for unsolicited inbound traffic. You can configure up to 48 rules: 24 each in Port Forwarding and Extended Port Forwarding.

You can also lock down network port access, either globally or by specific source addresses. You can specify individual addresses or address ranges.

All forwarding and filtering features are turned off by default.

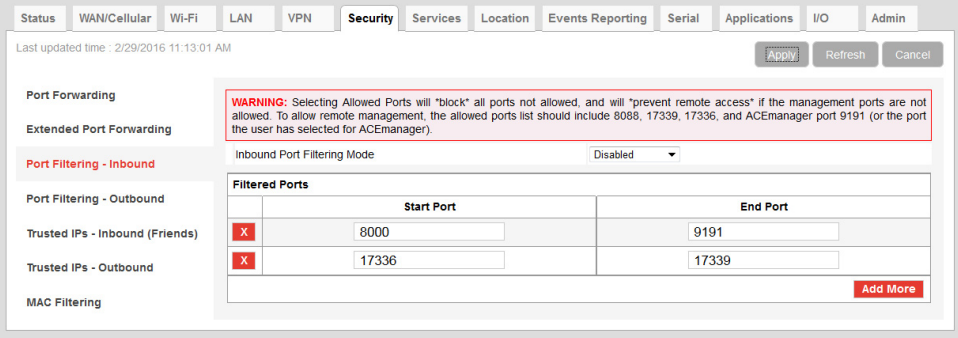


Figure 2-5: ACEmanager: Security > Port Filtering - Inbound

Device and Radio Module Firmware

Keeping your AirLink routers and gateway updated with new ALEOS and radio module firmware is an important part of overall system security.

New firmware is released to accomplish three main purposes:

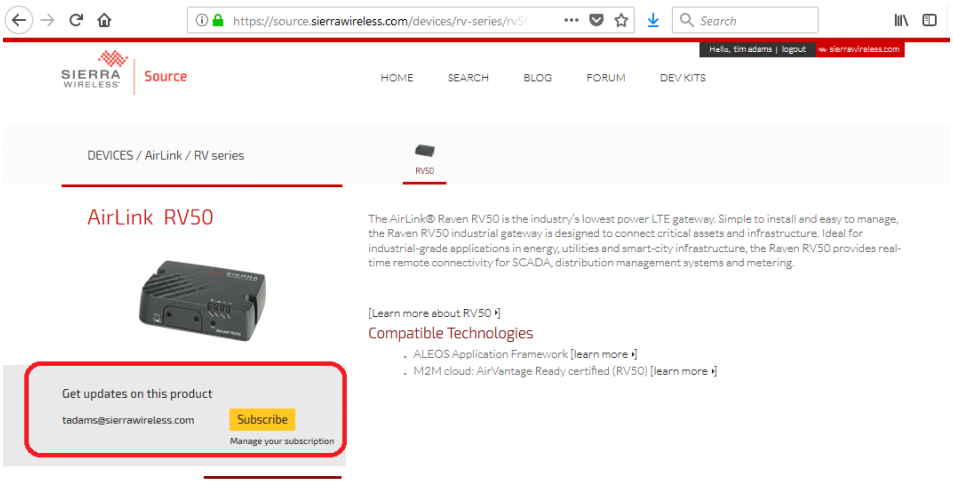
- Provide new features
- Support new hardware configurations and components
- Provide security patches for specific vulnerabilities

When a new ALEOS version is released, you should:

- Review the Release Notes to see what the release contains
- Evaluate your need for new features and risk tolerance for patches
- Load the new release on a test bench system, then a pilot group

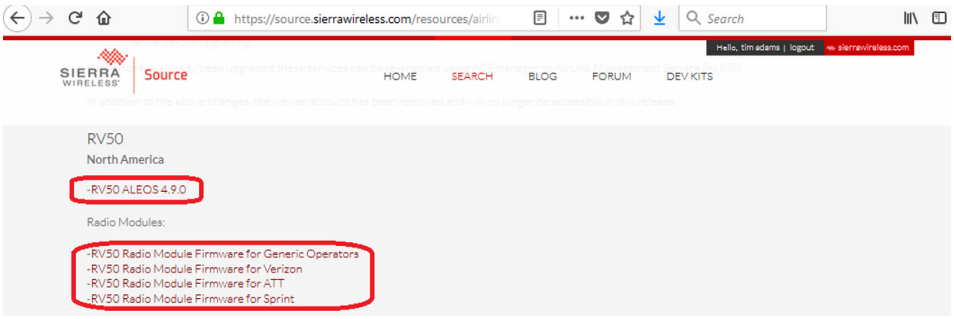
Sierra Wireless recommends subscribing to product updates on the Source. The Source is the Sierra Wireless technical library and self-serve portal for accessing documents and downloads. Please visit source.sierrawireless.com.

For products that you use, you can Subscribe so that you receive notifications when new releases and technical bulletins are released for your products.



On the Source, you will find ALEOS releases (for devices) and radio firmware for specific modems used in various devices.

Note: Radio module firmware is module and carrier-specific. Some versions of ALEOS expect certain versions of radio module firmware.



Sierra Wireless doesn't expect every customer to deploy every version of ALEOS that is released.

Considerations in upgrading even if your system performance is fine:

- Upgrading across many releases can be challenging, and not every path—upgrading from version x to version z, compared to from version y to version z, for example—can be tested
- New devices will be delivered with current production versions—it's usually better to upgrade than downgrade to have a consistent fleet
- New versions are often released on a 6-month cycle by design
- Carriers use new radio module firmware releases to maintain good access to their networks
- It's better to upgrade while it isn't broken than to wait until it is

Sierra Wireless recommends that you run your mission-critical device fleet on a release that is not more than two major releases old.

Two major releases provides significant time for evaluating a new release and deploying a version that passes internal testing and validation.

Using a management platform such as ALMS or AMM greatly simplifies firmware upgrading.

Important: *Sierra Wireless always recommends updating ALEOS to the latest version to take advantage of new features and security updates. If your application requires you to install an earlier version of ALEOS than your current version, please note that Sierra Wireless:*

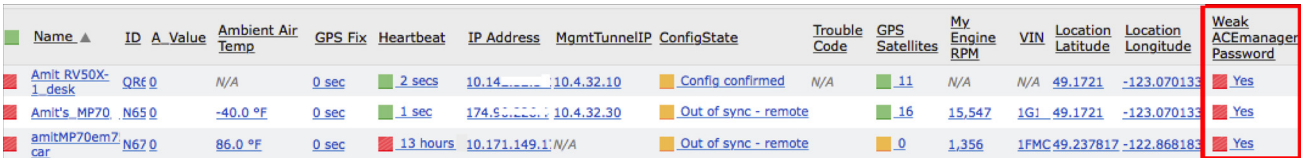
- *does not recommend using any version prior to ALEOS 4.9.3.*
- *recommends that ALEOS devices be reset to factory defaults following any downgrade operation.*

Note: ALEOS software releases may not apply to all AirLink devices. Please ensure that the version you select is compatible with your device.

Password Strength

Identifying the Strength of Passwords on ALEOS Devices

The Dashboard in AMM 2.16.2 and above includes a column entitled Weak ACEmanager Password that indicates whether or not the login password for an ALEOS device is weak. Note that the column won't show up for MGOS-only fleets:



Name ▲	ID	A_Value	Ambient Air Temp	GPS Fix	Heartbeat	IP Address	MgmtTunnelIP	ConfigState	Trouble Code	GPS Satellites	My Engine RPM	VIN	Location Latitude	Location Longitude	Weak ACEmanager Password
Amit RV50X-1_desk	QR6	0	N/A	0 sec	2 secs	10.14[illegible]	10.4.32.10	Config confirmed	N/A	11	N/A	N/A	49.1721	-123.070133	Yes
Amit's_MP70	N65	0	-40.0 °F	0 sec	1 sec	174.5[illegible]	10.4.32.30	Out of sync - remote		16	15,547	1G[illegible]	49.1721	-123.070133	Yes
amitMP70em7car	N67	0	86.0 °F	0 sec	13 hours	10.171.149.1[illegible]	N/A	Out of sync - remote		0	1,356	1FMC	49.237817	-122.868183	Yes

Figure 2-6: The "Weak ACEmanager Password" Column in the Dashboard

The value for the column will be set as follows:

- Yes: when an ALEOS password is set to one of 1,000,000 known weak passwords.
- No: the password is not set to one of the weak passwords, and is therefore considered strong.
- N/A: If multiple device types are selected, the column will be set to N/A for all non-ALEOS devices.
- HTTP: if the device is configured to communicate to the AMM over HTTP, rather than HTTPS, the column will be set to HTTP to indicate that the password state cannot be determined.

Note: Sierra Wireless does not recommend that devices communicate with management systems over insecure channels. HTTPS should be used.

Note: The value of the column is updated when an ALEOS device checks in. However, if the weak password was fixed on ACEmanager, the value won't be updated automatically; in this case the "Revert" button on Configuration -> Deploy page must be clicked.

3: Service Security

Using a management system is a best practice when it comes to system security. A management system such as AirLink Management Service (ALMS) or AirLink Manager/ AirLink Mobility Manager (AM/AMM) will monitor your system activity and provide your enterprise with improved functionality and insights, thereby better securing your devices.

ALMS features interactive monitoring dashboards and maps that show the status, signal strength, data usage and location of all registered AirLink gateways. If this information indicates malicious activity, your enterprise can then take action to fend off an attack or recover from a successful breach.

AirLink Management Service and AirLink Manager/AirLink Mobility Manager also give you control over device configuration and software updates, making it easier for your enterprise to provide devices with security updates, bug fixes and new security measures.

AirLink Management Service provides a one-to-many solution for both monitoring the status of all your devices as well as configuring all of your devices. It is the preferred way for customers to upgrade their firmware and embedded application over the air. The firmware is delivered automatically to customers via AirVantage, and can be applied to all or selected group of devices easily.

Defense in Depth Device Strategy

An effective security strategy employing AirLink management systems encompasses the following elements:

- ❑ Disabling unused services
  - Use a management system to disable remote access to ACEmanager, for example
  - Disable ALMS itself if you do not need to use it
- ❑ Limiting access to enabled services
  - Restrict login by IP (see User IP filtering on page 21)
  - Limit/audit user accounts
- ❑ Managing and Strengthening Authentication
  - ALMS can enforce 2-factor authentication (see Two-factor authentication on page 20)
- ❑ Limiting Authenticated Actions
  - Use different user types (see Managing Administrators on page 22)
- ❑ Detection
  - Audit user activity

Public IP vs Private IP

AirLink Management Service does not require your devices to have public IP addresses. Unlike most device management applications, AirLink Management Service has been designed to support a device-initiated communication model. This allows your devices to remain privately secured behind your firewall (or your network operator's firewall) and still communicate with AirVantage.

AirVantage can work with operator private networks. It is simply a matter of configuring your network to allow management traffic to AirVantage. Remember, you need only allow outgoing traffic because of ALMS's device-initiated communication model. You can maintain all inbound firewall protection.

Recommendations When Using ALMS

Sierra Wireless recommends registering your AirLink routers in ALMS, irrespective of your plans to use ALMS for device management. Registration claims the device into an account you manage and can easily mitigate any security issues around improper authentication. Registration also provides an easy way to track warranty and support information for your devices.

For devices purchased within the last 60 days, registering the device in ALMS will register the device and activate AirLink Complete. This provides access to ALMS, Customer Support and Warranty and is included at no cost for the first year after activation. At the end of the first year the devices will automatically move to the inventory state and be suspended in ALMS if the service is not explicitly renewed or extended.

If your device was purchased more than 60 days ago Sierra Wireless still recommends creating an account and registering your devices. Registering the device in ALMS will place it into an inventory state. The device will be associated with the account but will not be active in the system or incur any cost until you chose to activate it. Devices in the inventory state can be activated at any time with the appropriate service (such as AirLink Complete). Please speak to your Sierra Wireless Partner to purchase services for older devices.

To create a new ALMS account please visit the ALMS registration page.

Disable the ALMS Service in the Device

If you are unable to register their devices in ALMS, Sierra Wireless recommends disabling the service on your devices. This prevents the devices from communicating with ALMS. Do this only if you know the device will never need remote management in the future.

Please note that you will need to manually reconfigure each device locally if you ever need to re-enable access to ALMS in the future.

To disable ALMS access:

1. In AceManager, go to Services > ALMS (see Figure 3-1 on page 19).
2. Set ALMS Protocol to Disable and apply the settings.

Note: This setting will need to be updated in the future if ALMS support is desired.

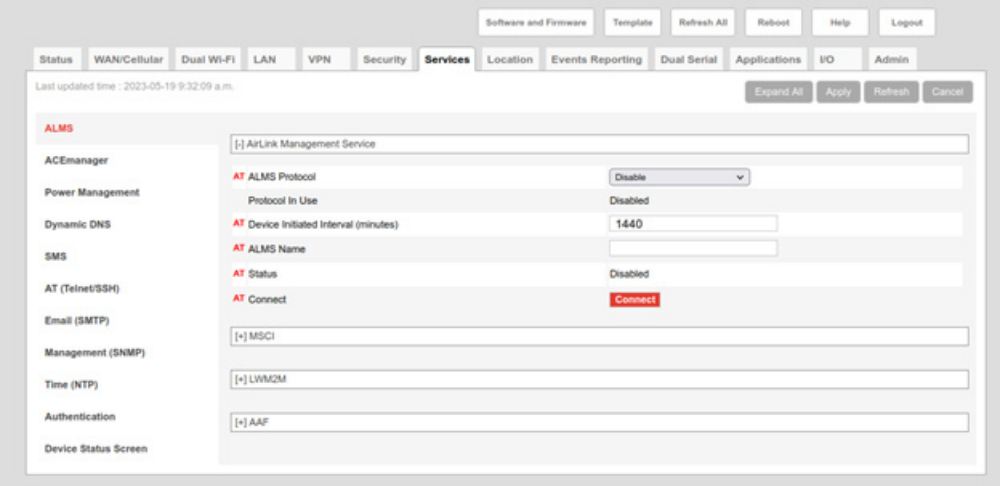


Figure 3-1: ACEmanager Services > ALMS

Managing Credentials Using ALMS

Apply Settings

Accessed from the action buttons on the Monitor > Systems page, the Apply Settings feature allows you to update settings such as the ACEmanager Password and Wi-Fi pre-shared keys with the same value or unique values, on multiple systems.

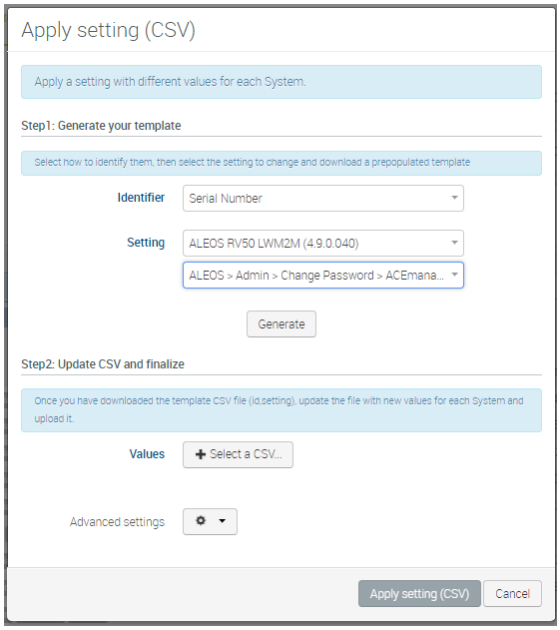


Figure 3-2: Apply setting template

ALMS Security Options

The security options described hereafter are based on user or device connection restrictions. Those options are configurable per company. These restrictions help protect your data from unauthorized access and phishing attacks. The Security section in ALMS also covers the management of company administrators.

To access the security section, from My Account click on Administration > Security:

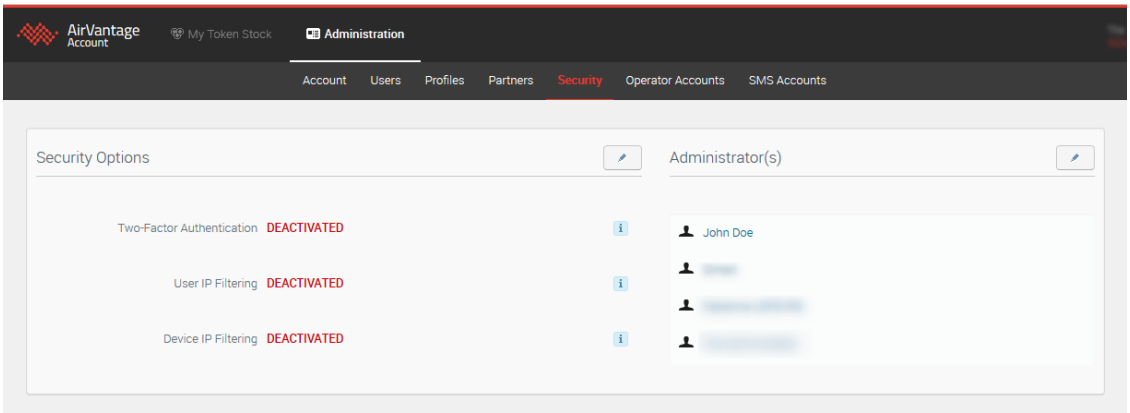


Figure 3-3: Administration > Security

Two-factor authentication

The two-factor authentication (2FA) option enables two-stage verification to double check the identity of a user trying to log in to ALMS. It combines the standard login based on a user name and password (“something the user knows”) with an additional factor (“something the user has”).

When this option is activated, after entering credentials on the login page, the user will have to provide the 6-character code (a one time password) the user will receive by SMS on their phone. The SMS is sent by ALMS to the phone number configured in the user’s detail form. This 2FA will be required at every log in for every user of the company.

For the 2FA feature to operate correctly, all users in the company MUST have a phone number in their user profile. In addition, once 2FA is activated in the company, all new users will require a phone number.

Note: To enable two-factor authentication in your company, please contact your Sierra Wireless partner or our support team.

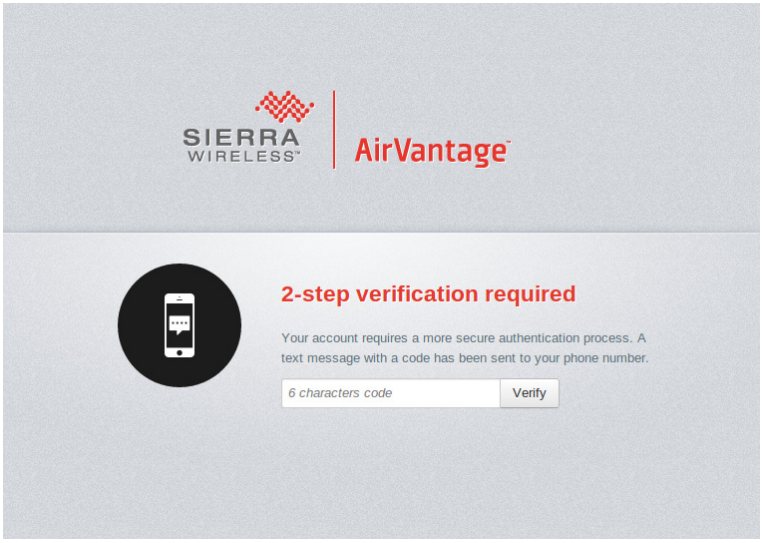


Figure 3-4: 2-step verification

User IP filtering

The User IP filtering option enables you to restrict users login based on the IP addresses they are logging from. You can therefore use this option and configure it with your organization trusted IP Range.

As input, you can provide:

- A range of IP
- And/Or a list of IP

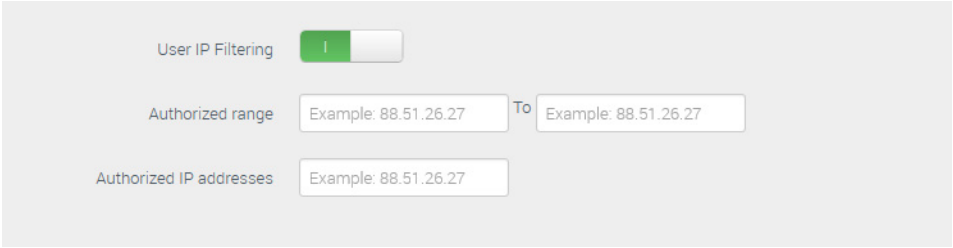


Figure 3-5: User IP Filtering

Once the option is activated, a user trying to log from an IP address not in the authorized list will be denied access to ALMS.

Device IP filtering

The Device IP filtering option enables you to filter devices access based on the IP addresses they communicate from. You can therefore use this option and configure it with your organization's trusted IP Range.

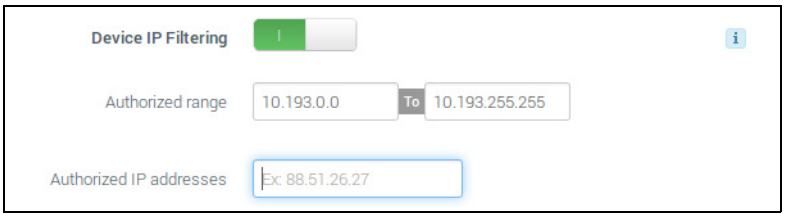


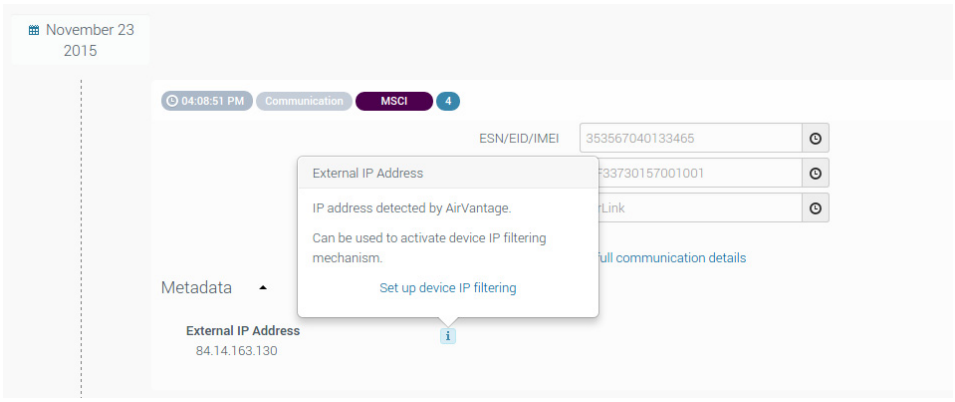
Figure 3-6: Device IP filtering

As input, you can provide:

- A range of IP
- And/Or a list of IP

If your devices are communicating through a VPN to ALMS, you should use the range **10.191.0.0** to **10.191.255.255** for NA and **10.193.0.0** to **10.193.255.255** for EU to ensure every device communication comes from within the VPN.

If you are not using a VPN to ALMS, you can still use this option. As the IP address allocated to devices depend on your operator, to help you with the configuration of the option, you can find the external IP address detected by ALMS for each system in the timeline of this specific System.



Once the option is activated, a device trying to communicate from an IP address not in the authorized list will be denied access to ALMS.

Managing Administrators

Company administrators are the only ones who can edit the security configuration, create new users or profiles.

An administrator can promote any user from the company, and also add users from partner companies to the role of company administrator: choose the partner click in the Administrators field to select users from the partner.

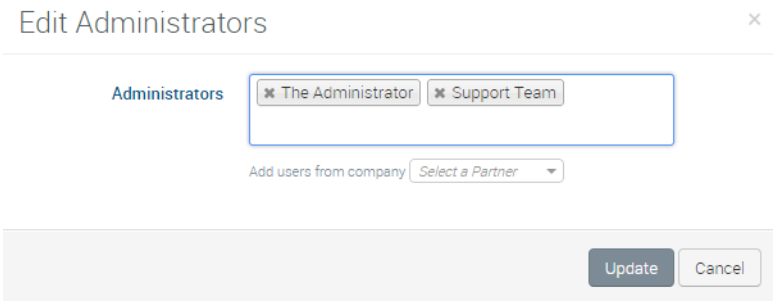


Figure 3-7: Edit Administrators

Account timeouts on incorrect user authentication

AirVantage requires the user to authenticate with the system to provide access. As part of the standard security options AirVantage prevents users from making multiple erroneous login attempts. The system requires a user to wait a random, exponentially increasing amount of time between unsuccessful login attempts. This prevents automated systems from attempting to brute force user passwords.

In addition to preventing this incorrect login attempts, the system also records all login attempts, both successful and failures. There is an API that users can call to access the log of these attempts.

AMM Security Features

Managing Credentials Using AMM

The AMM enforces security by requiring each user to log in with a name and password.

To safeguard your login credentials, ensure that your browser does not store your user name and password unless you are confident that no one can access your computer.

Note: The system will log out the current user after 30 minutes of browser inactivity.

Options > Preferences allows the system administrator to set user password and remote authentication, as well as Read/Write privileges for users.

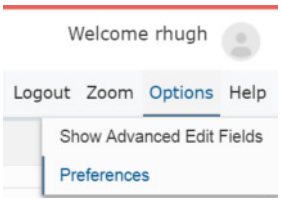


Figure 3-8: AMM > Options > Preferences

Remote Access

AMM Total Reach feature: Total Reach allows users of the AMM to remotely access a device (e.g. laptop, handheld, etc.) in a gateway's LAN or Vehicle Area Network (VAN) via the AMM. System administrators can control which users are granted Total Reach privileges. Note that Total Reach enables access to specific services (VNC, HTTP/HTTPS, SSH) running on the device. If you wish to limit access to a device by users with the Total Reach privilege, ensure any unnecessary services are disabled on the device and/or ensure authentication requirements are in place for enabled services.

Deleting Information from a Hosted AMM

Any user who is an authorized Customer Support Contact in the Sierra Wireless Support Portal can request to delete their users' personal data from a hosted AMM. While a hosted AMM stores very limited personal information, the ability to delete a person's personal information allows companies to meet the European Union's General Data Protection Regulation (GDPR).

To begin this process, an AMM user who is an authorized Customer Support Contact in the Sierra Wireless Support Portal must ask their Customer Support Contact to delete their profile information. The Customer Support Contact will then open a ticket on the Customer Support Portal on the user's behalf.

Sierra Wireless will then remove the following:

- Display name
- Email address
- Last login location (IP address)

To preserve the history of the AMM and to prevent confusion for other users, the history of user activity in the User Activity report won't be deleted and their generated reports will remain on the AMM.

Software Updates

As a best practice, Sierra Wireless recommends that you run your mission-critical device fleet on a release that is not more than two major releases old. Two major releases provides significant time for evaluating a new release and deploying a version that passes internal testing and validation.

New firmware provides new features, supports new hardware configurations and components, and provides security patches for specific vulnerabilities. Using a management platform greatly simplifies firmware upgrading.

For information about using ALMS to upgrade firmware for your ALEOS gateways and routers, see the how-to article How to upgrade firmware on my ALEOS gateways.

For information about using AM/AMM to upgrade firmware, see the AMM Operation and Configuration Guide (Admin Tab > Software section).

4: Appliance Security

AirLink Connection Manager (ACM) is a WAN-based VPN software application (available in VMWare or appliance form factor) designed to work with Sierra Wireless AirLink gateways and routers. ACM provides security for all connected devices and applications in the router or gateway's "vehicle area network".

AirLink Connection Manager Security Features

Administrator Password

ACM has a default password that should be changed on first login. To change the default password of the admin account, use the following commands:

```
admin@ACM:~# set system login user admin authentication plaintext-password <PASSWORD>
admin@ACM:~# commit
```

Note: Once the change is committed, the password is encrypted and is no longer available in plain text.

VPN Configuration

For a comprehensive guide to VPN configuration in ACM, refer to the ACM Installation and Operations User Guide (Document #4111747), available on the ACM device page at source.sierrawireless.com.

Considerations for ACM selection and configuration include:

- Virtual vs Physical Appliance—Installing the ACM as a physical appliance requires secure installation practices, the same as other data center appliances.
- FIPS Compliance
- High Availability (HOT/WARM and HOT/HOT)—see the High Availability Configuration Guide (Document #4118775), available on the ACM device page at source.sierrawireless.com.
- Certificate-based Client Authentication
- Global Firewall Rules
- Split vs Full Tunnel
- Address Space, DNS, and NTP Configuration
- WAN address dynamic IP addressing

Windows/Android Client Configuration

In addition to support for AirLink gateways and routers, ACM also supports the NCP Secure Entry Client for Windows and Android. For details, refer to the AirLink Connection Manager Configuration Guide for NCP Secure Entry Client (Document #4118774), available on the ACM device page at source.sierrawireless.com.