SIERRA WIRELESS IS NOW SEMTECH®

AirLink

AirLink Connection Manager (ACM)

Installation and Operations Guide

August 2024

41111747 Rev. 9

Important Notice

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

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

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

Wireless Communications

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

Warranty

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

Safety

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

Sierra Wireless

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

Contact Information

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

Revision History

Revision number	Release date	Changes
1	December 2017	▪ Document created
2	July 2018	▪ Updated Table 5-8 with information about RFC7427 for NCP 10.1 clients and information about IKEv1 support ▪ Added Global Firewall Rules topic and corresponding entry in Configure VPN Peer Attributes
3	October 2019	▪ Updated ACM appliance version
3.1	January 2023	▪ Updated Virtual Machine Server Specifications to match rev.5
4	November 2022	▪ Replaced Vyatta with VyOS ▪ Updated Table 1-1 Supported Embedded Software Versions ▪ Removed Physical ACM Appliance Requirements (bare metal option for initial deployment) ▪ Added XR series routers ▪ Added RX55 router ▪ Removed LS series gateways ▪ Updated document for ACM 2.2 non-FIPS, including: · Upgraded to Debian 10. · Added XR series routers · Updated cryptographic suite for compatibility with AirLink OS 3.1 (XR and RX series) — updated Table 5-1, Table 5-3, Table 5-4, Table 5-8; added Table 5-7
5	December 2022	▪ Updated Virtual Machine Server Specifications
6	May 2023	▪ Updated document for ACM 3.0 FIPS, including: · Upgraded to Ubuntu 20.04.5 LTS · Updated ACM 3.0 FIPS content in Table 5-1, Table 5-3, Table 5-4, Table 5-8; added Table 5-7

Revision number	Release date	Changes
7	June 2023	▪ Updated document for ACM 3.0 non-FIPS — Replaced ACM 2.2 (non-FIPS) references with ACM 3.0 (non-FIPS) in: · FIPS-Compliant ACM, Identifying ACM Configurations (FIPS vs non-FIPS), ACM Virtual Machine Deployment, Upgrading to ACM 3.1 (non-FIPS) or ACM 3.1 (FIPS) · Table 1-2, Table 5-1, Table 5-3, Table 5-3, Table 5-7, Table 5-8 ▪ Added Hardware and VM Server Requirements
8	June 2024	▪ Updated document for ACM 3.1 (FIPS and non-FIPS) ▪ Upgraded to Ubuntu 20.04.6 LTS ▪ Added SNMP Remote Management ▪ Added Remote Logging (Syslog) Setup
9	July 2024	▪ Updated document for ACM 3.1.1 (FIPS and non-FIPS) ▪ Updated ACM Virtual Machine Deployment (specify standalone server) ▪ Updated Virtual Machine Server Specifications ▪ Updated SNMP Remote Management (SNMP version support) ▪ Updated Upgrading to ACM 3.1.1 (non-FIPS) or ACM 3.1.1 (FIPS) (ACM version number, .iso filename)

Contents

1: Introduction

This document provides configuration instructions for the AirLink Connection Manager (ACM) VPN appliance.

Tip: *To find all ACM-related documents, click the "Find more resources" link on the ACM device page on the Source (source.sierrawireless.com/devices/airlink-vpn/acm-vpn-server).*

Who Should Read This Guide

ACM users typically include IT support staff and IT security staff.

What is AirLink Connection Manager?

ACM is a VPN appliance available as a virtual machine (VM) on VMWare vSphere ESXi.

ACM is designed to work with Sierra Wireless' AirLink routers. ACM provides security for all connected devices and applications in the router's "vehicle area network".

Figure 1-1 shows how ACM fits into a standard enterprise deployment:

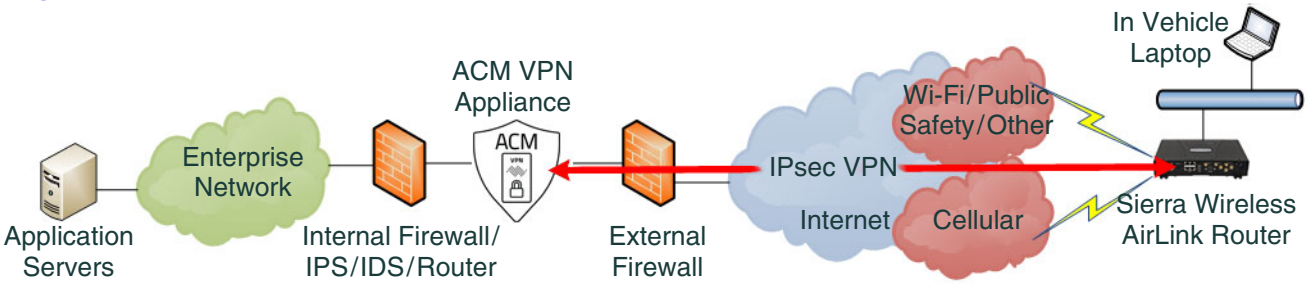


Figure 1-1: ACM fits between firewalls in an enterprise deployment

ACM eliminates session interruptions when secure IP traffic is switched from one wireless network to another because it is based on IKEv2 Mobile Internet Key Exchange (MOBIKE) standards. On AirLink routers that support IKEv2, MOBIKE enables the device to establish a secure tunnel over any available wireless network, and as the vehicle moves and network access changes, the router can "move the tunnel" to the next best available network. This happens automatically, transparently, and without disruption to the end-user's applications.

Note: IKEv2 is supported on oMG2000/500 and MG90 routers, NCP Client for Windows, XR series routers, and AirLink devices running ALEOS 4.12.0 or later.
It is not supported on AirLink devices running ALEOS 4.9.x or earlier.

The ACM is based on proven VyOS technology and strongSwan (for more information, go to https://www.vyos.net and https://www.strongswan.org/).

Note: The ACM supports a subset of the commands and attributes described in the VyOS Configuration Guide's VPN section (https://docs.vyos.io/en/equuleus/configuration/index.html).

SNMP Remote Management

ACM 3.1.1 supports SNMP remote management.

Important: *ACM 3.1.1 (FIPS/non-FIPS) supports only SNMPv2c. SNMPv3 is not supported.*

The ACM 3.1.1 Management Information Base (MIB) includes the following managed objects:

Table 1-1: SNMP MIB Objects

OID	Object
system (OID: .1.3.6.1.2.1.1)	sysname: ACM
	sysUpTime
interfaces (OID: .1.3.6.1.2.1.2)	ifNumber: 3
	ifDescr 1: lo
	ifDescr 2: Broadcom
	ifDescr 3: Broadcom
	ifType
	ifMtu
	ifSpeed
	ifPhysAddress
	ifAdminStatus
	ifOperStatus
	ifLastChange
	ifInUcast Pkts
ip (OID: .1.3.6.1.2.1.4)	ipInReceive
	ipInDelivers
	ipOutRequests
	ipAdEntAddr: Eth0_IP
	ipAdEntAddr: lo
	ipAdEntAddr: Eth1_IP
icmp (OID: .1.3.6.1.2.1.5)	icmpInErrors
	icmpEchoReps
tcp (OID: .1.3.6.1.2.1.6)	tcpMaxConn
	tcpActiveOpens
udp (OID: .1.3.6.1.2.1.7)	udpLocal Port

FIPS-Compliant ACM

ACM 3.1.1 is available in non-FIPS and FIPS-compliant configurations, based on Ubuntu 20.04.6 LTS:

- The FIPS-compliant ACM 3.1.1 (FIPS) provides improved encryption capabilities and meets the requirements of the Federal Information Processing Standard 140-2, security level 1, using FIPS 140-2 certified packages available with Ubuntu Pro (https://ubuntu.com/security/fips).
- ACM 3.1.1 (non-FIPS) addresses security vulnerabilities from ACM (non-FIPS) 3.0.

Identifying ACM Configurations (FIPS vs non-FIPS)

Several methods can be used to confirm if the ACM is a FIPS or non-FIPS configuration.

(Note — The responses shown below for each method are examples only.)

- Method 1 — Enter the following command. The response shows the kernel version, and will show "-fips" if the ACM is a FIPS configuration.
  - ACM 3.1.1 (FIPS) or later — In this example, the response shows that the kernel version is 5.4.0-1095, the system is a FIPS configuration ("-fips" parameter), and the OS is Ubuntu:

    ```
    admin@ACM:~$ uname -a
    Linux ACM 5.4.0-1095-fips #105-Ubuntu SMP Mon Mar 11 14:17:14 UTC 2024
    x86_64 x86_64 x86_64 GNU/Linux
    ```

  - ACM 3.1.1 (non-FIPS) or later — In this example, the response shows that the kernel version is 5.4.0-176-generic, the system is a non-FIPS configuration (no 'fips' parameter), and the OS is Ubuntu:

    ```
    admin@ACM:~$ uname -a
    Linux ACM 5.4.0-176-generic #196-Ubuntu SMP Fri Mar 22 16:46:39 UTC 2024
    x86_64 x86_64 x86_64 GNU/Linux
    ```

- Method 2: — Enter the following command to check if FIPS is enabled. FIPS is enabled if the response is "1".

  ```
  admin@ACM:~$ cat /proc/sys/crypto/fips_enabled
  1
  ```

- Method 3: — Enter the following command to display the openssl library used with the FIPS ACM:

  ```
  admin@ACM:~$ OPENSSL_FIPS=1 openssl version
  FIPS mode is always enabled, ignoring OPENSSL_FIPS.
  OpenSSL 1.1.1f  31 Mar 2020
  ```

- Method 4: — Enter the following command to display the FIPS ciphers that are supported by openssl:

  ```
  admin@ACM:~$ openssl ciphers FIPS
  TLS_AES_256_GCM_SHA384:TLS_CHACHA20_POLY1305_SHA256:TLS_AES_128_GCM_-
  SHA256:ECDHE-ECDSA...
  ```

Supported VPN Peers (Endpoints)

VPN peers supported by ACM include AirLink routers and the NCP Secure Entry Client for Windows.

Note: The term "VPN peer' is used in this document to refer to VPN clients (endpoints).

ACM FIPS and non-FIPS releases are supported on the following configurations:

Table 1-2: Supported Embedded Software Versions

Platform	Embedded Software	
	ACM 3.1.1 (Non-FIPS)	ACM 3.1.1 (FIPS)
MG90	MGOS 4.3 or later	
oMG500/oMG2000	MGOS 3.15.x	
LX40, LX60, MP70, RV50, RV50X, RV55	ALEOS 4.14 or later	
ES450, GX450	ALEOS 4.9.x	
NCP Secure Entry Client	NCP 13.11 (Tested)	
RX55, XR60, XR80, XR90	AirLink OS 4.0.23 or later	

Supported Mobile Client (NCP Client for Windows)

ACM 1.6 and later supports connections from systems using NCP Secure Entry Client for Windows. 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/devices/airlink-vpn/acm-vpn-server/.

2: Installation

This chapter describes how to install (deploy) a new ACM 3.1.1 (FIPS) or ACM 3.1.1 (non-FIPS) virtual machine (VM) on a VMWare vSphere server, and connect ACM to your network.

To upgrade an existing ACM 2.1 (FIPS), ACM 2.2 (non-FIPS) or ACM 3.0 (FIPS/non-FIPS) VM to ACM 3.1.1, see Upgrading to ACM 3.1.1 (non-FIPS) or ACM 3.1.1 (FIPS) on page 55.

ACM Virtual Machine Deployment

The ACM 3.1.1 (FIPS) and ACM 3.1.1 (non-FIPS) VMs have been tested for deployment on a VMWare vSphere ESXi 7.0+ (ESXi) standalone server that has been configured as required for use with ACM.

Note: To deploy ACM 3.1.1 (FIPS or non-FIPS) on an earlier vSphere ESXi version, the ACM 3.1.1 (FIPS) or ACM 3.1.1 (non-FIPS) .iso file must be used. If an .ova file installation is required, refer to VMware documentation (https://docs.vmware.com) to generate and deploy an .ova file for ESXi 6.0, ESXi 6.5 or ESXi 6.7.

Virtual Machine Server Specifications

For ACM to provide reasonable performance, the ESXi server device must meet the following minimum specifications (to support up to 1000 concurrent active tunnels with a tunnel creation rate of 100 tunnels/min):

- vCPU cores: 8 dedicated cores
- vRAM size: 16 GB
- Available hard disk space: 16 GB

Note: To support larger numbers of concurrent tunnels, additional vCPU cores, vRAM, and hard disk space will be required.

Before deploying the ACM VM, you will need the following information from the ESXi server:

- IP address for the vSphere Hypervisor client on the server
- vSphere Hypervisor username and password
- Inside and outside network adapter names

Note: If high availability is required, refer to ACM Server High Availability on page 44 for details.

Note that when deploying an ACM VM in a VMware cluster environment:

- Semtech strongly recommends binding the VM to a single physical host to avoid instability and traffic disruption.
- Live VM migrations are not supported. ACM VM migrations should be performed by shutting down the VM, exporting it, and then importing it into the new ESXi server.

Deploying ACM VM From OVA File

Note: For detailed information about VMWare ESXi 7.0+, refer to documentation provided by VMWare.

To deploy an ACM VM on the ESXi 7.0+ server, using an .ova file:

1. Download the ACM .ova file. (Contact your Sierra Wireless Support representative for instructions on downloading the file.)
2. On a Windows or Mac computer (Linux is not supported), open a browser and then connect to the vSphere Hypervisor client's IP address (for example, https://10.10.10.10). The vSphere Hypervisor client will appear.

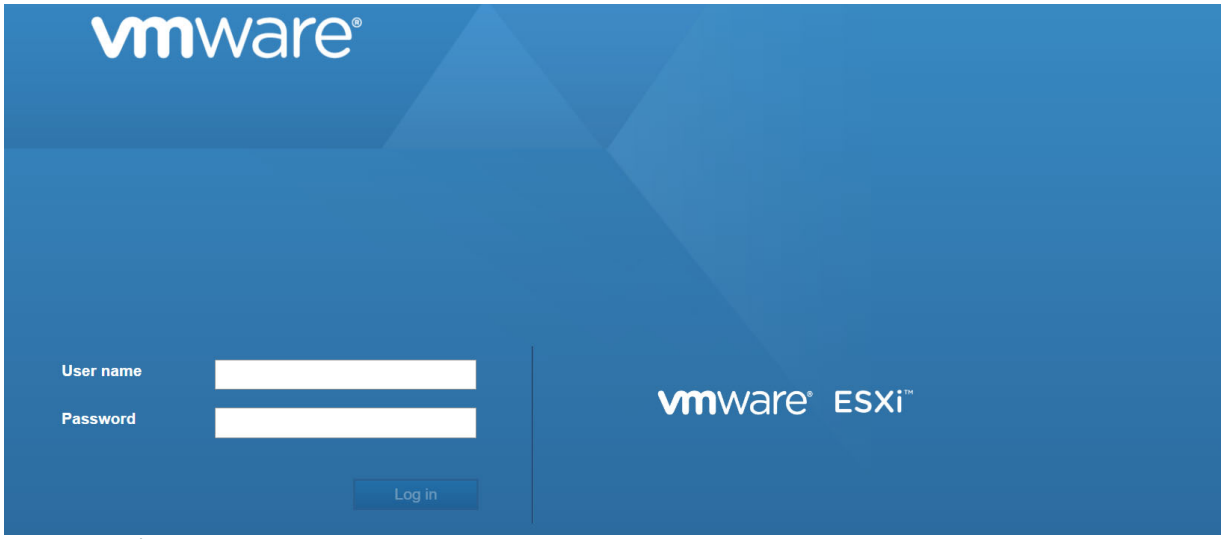


Figure 2-1: vSphere Hypervisor Login Screen

3. Enter the vSphere Hypervisor User name and Password, and click Log in. The vSphere Hypervisor interface appears.

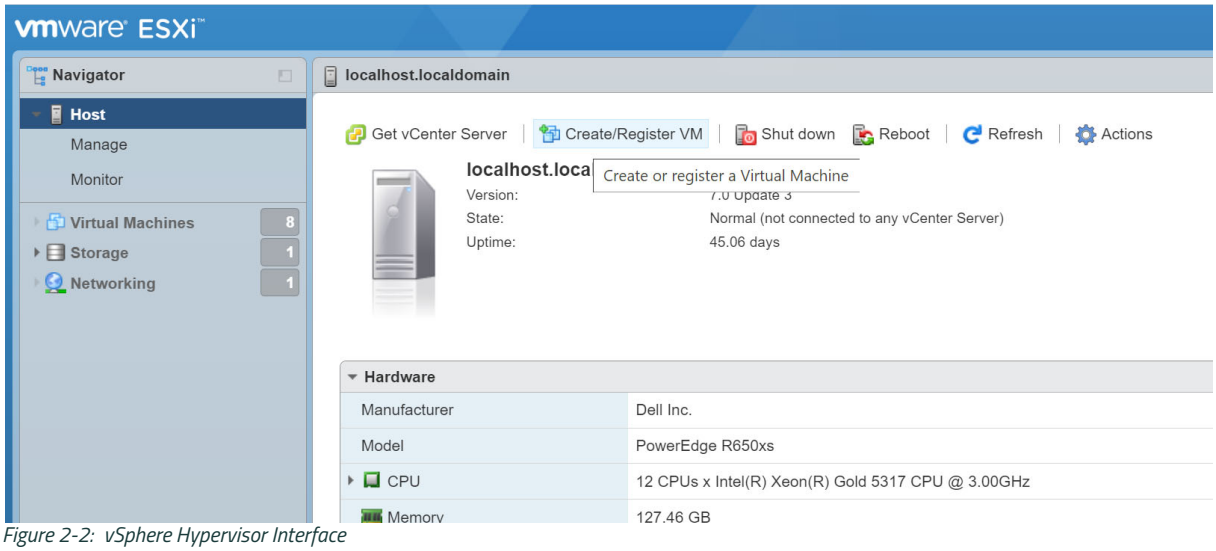
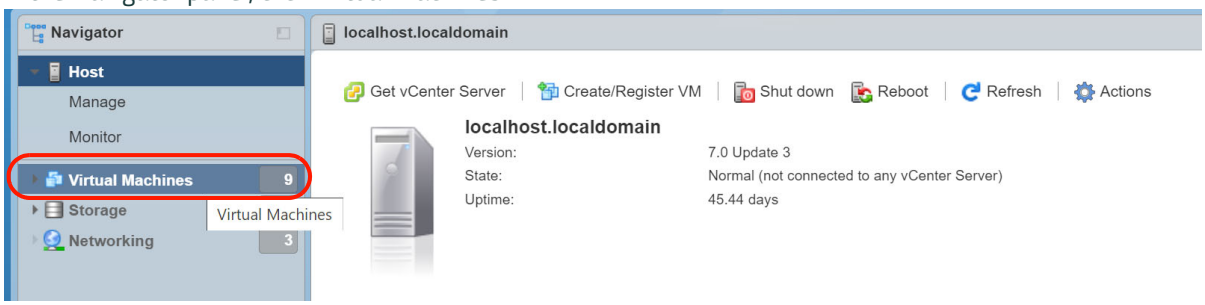
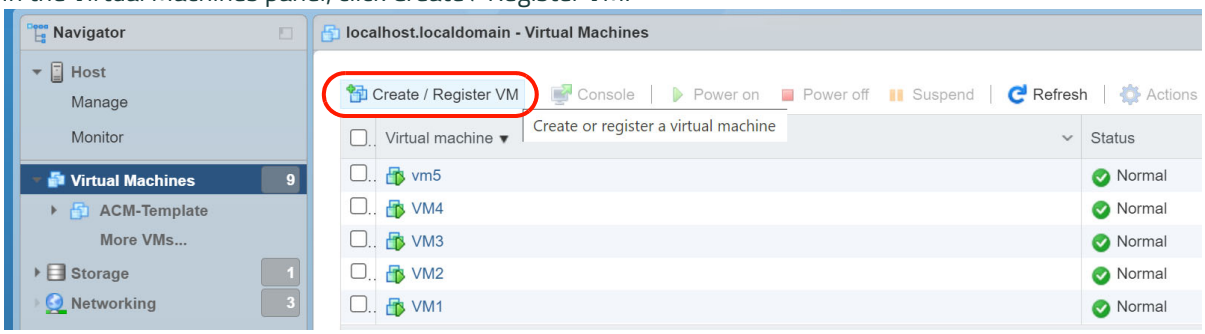


Figure 2-2: vSphere Hypervisor Interface

4. Create a VM:
   a. In the Navigator panel, click Virtual Machines.

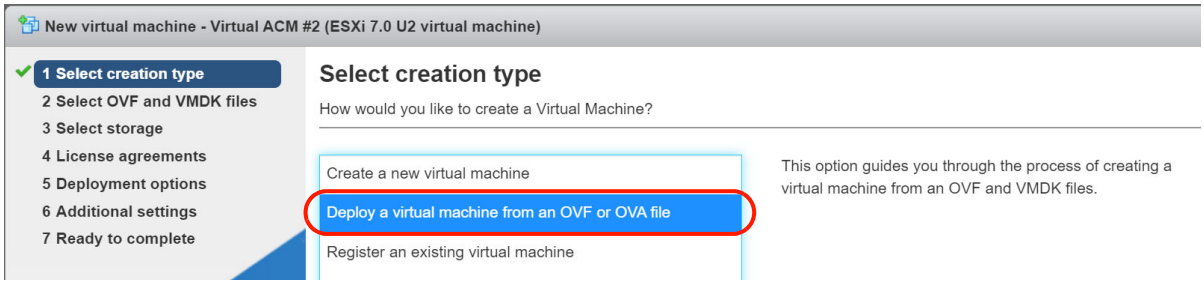


   b. In the Virtual Machines panel, click Create / Register VM.



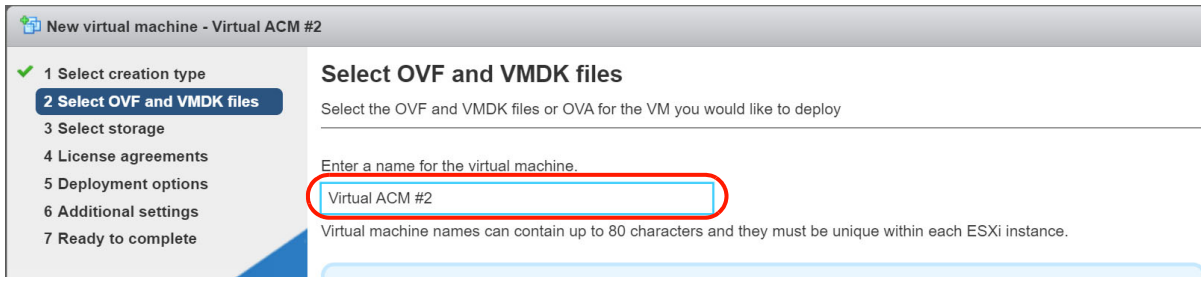
   The New Virtual Machine wizard appears.

   c. In the Select creation type panel, select Deploy a virtual machine from an OVF or OVA file.

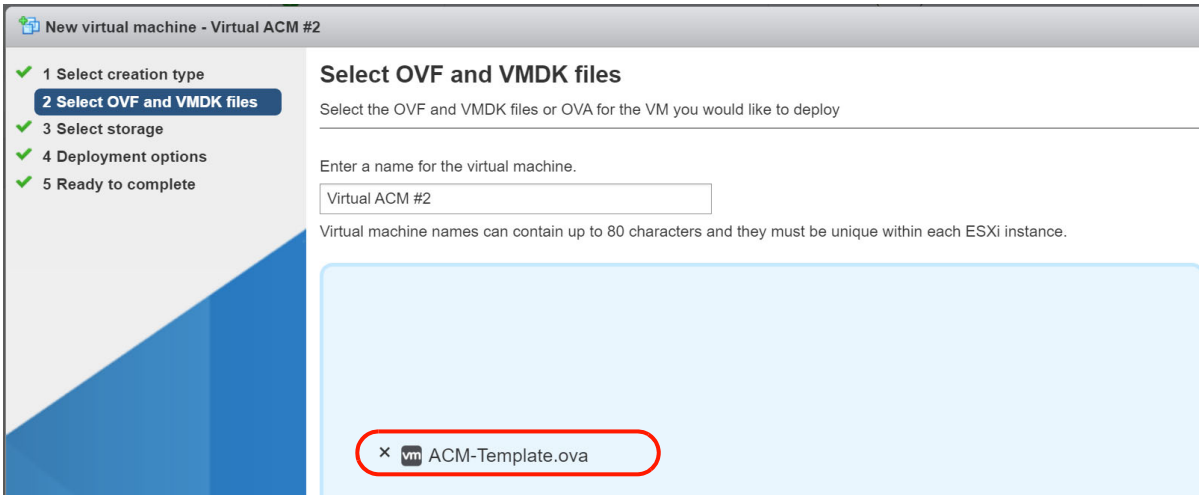


   d. Click Next.

   e. In the Select OVF and VMDK files panel, enter a name for the virtual machine. (For example: “Virtual ACM #2”.)

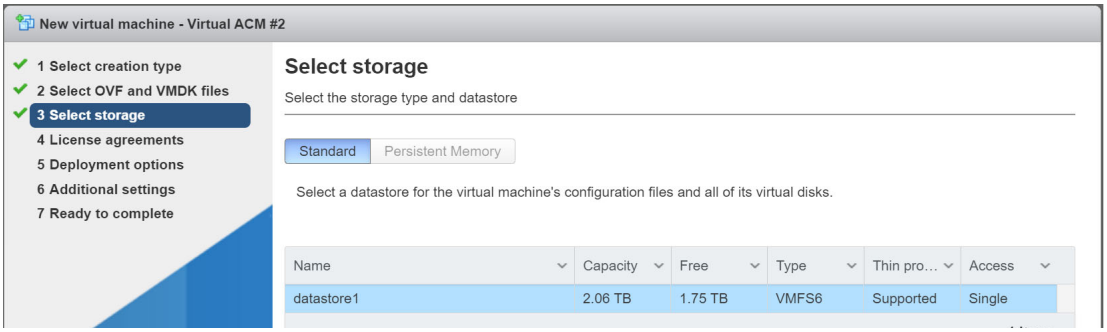


f. Click in the selection area to browse to (and select) the .ova file that you downloaded from Support, or drag and drop the .ova file into the selection area.



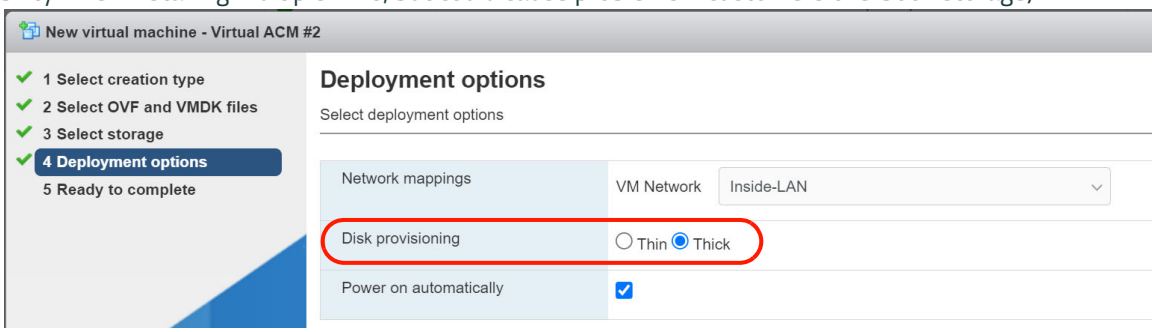
g. Click Next.

h. In the Select Storage panel, no changes are needed. Click Next.



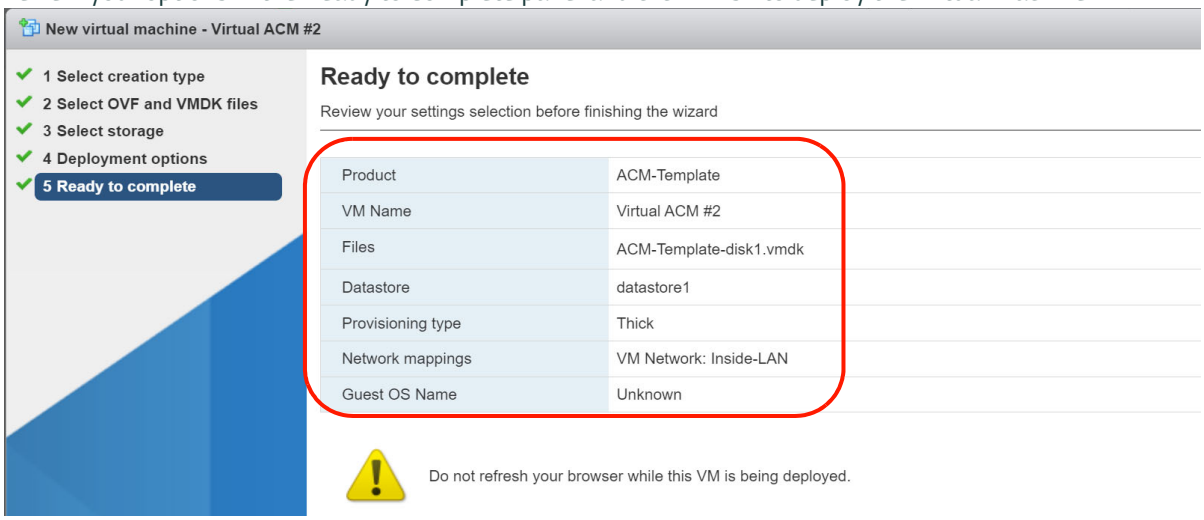
i. In the Deployment options panel, select the Disk provisioning method:

- Thick (recommended) — Fully allocates disk storage space so there is no concern with overbooking storage when installing multiple VMs.
- Thin — Allocates minimal disk storage space, and grows as the ACM uses space. Allows greater flexibility when installing multiple VMs, but could cause problems if customers overbook storage).

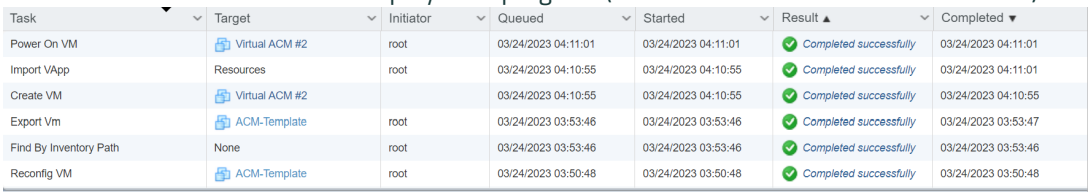


j. Click Next.

k. Review your options in the Ready to Complete panel and click Finish to deploy the virtual machine.

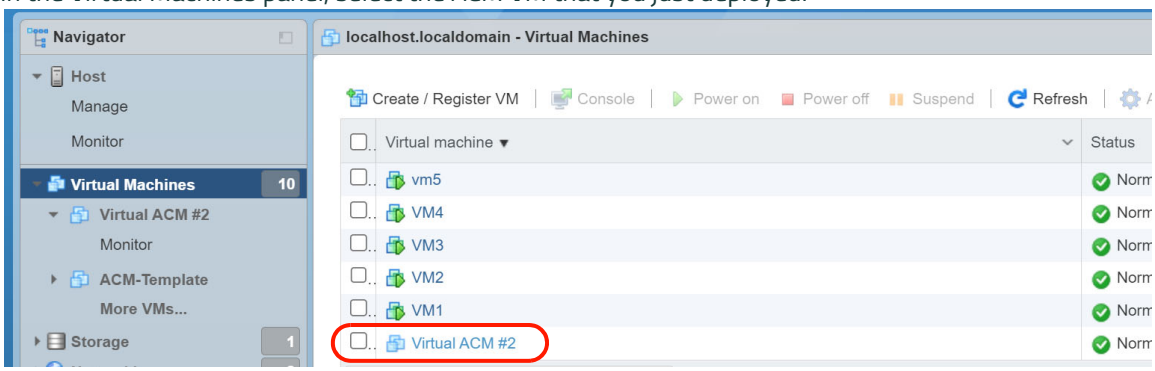


l. Wait for the ACM VM to deploy — Do NOT close the browser while it is deploying. The status area at the bottom of the screen shows the deployment progress (this will take at least several minutes.)

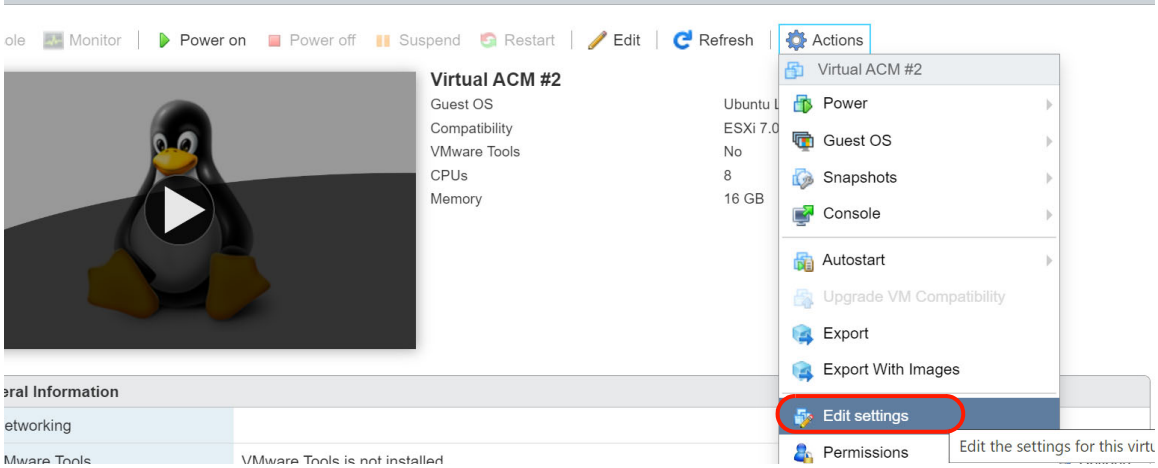


m. Add network adapters for the outside (eth0) interface and the inside (eth1) interface:

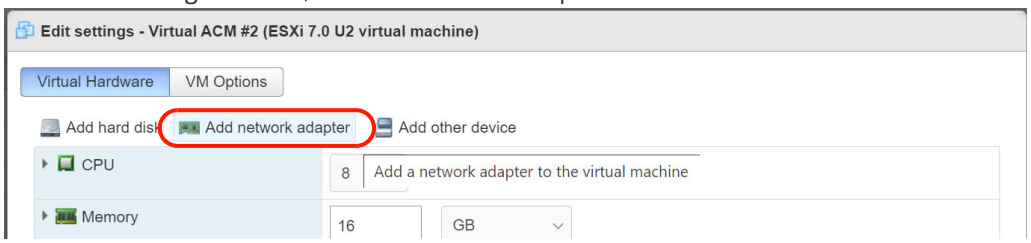
i. In the Virtual Machines panel, select the ACM VM that you just deployed.



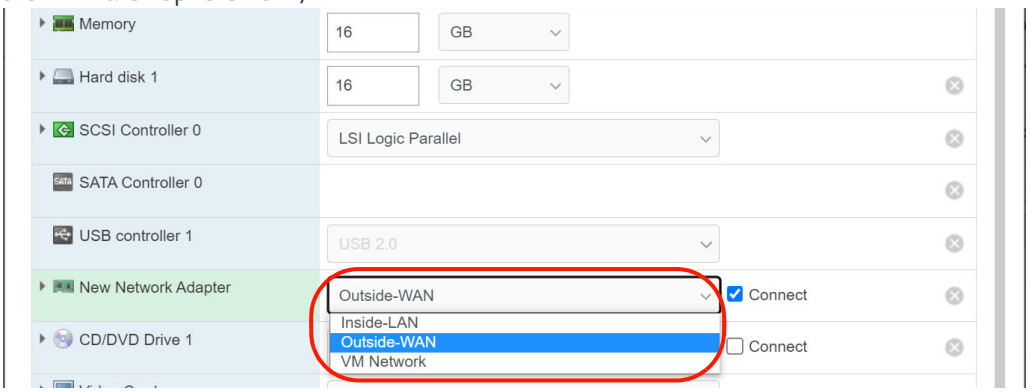
ii. Select Actions > Edit Settings.



iii. In the Edit settings window, click Add network adapter.



iv. In the New Network Adapter list, select the adapter to use for the outside interface (eth0), which is the WAN (Internet)-facing network. (The adapter names show are whatever were created by the installer of the VMWare vSphere ESXi.)

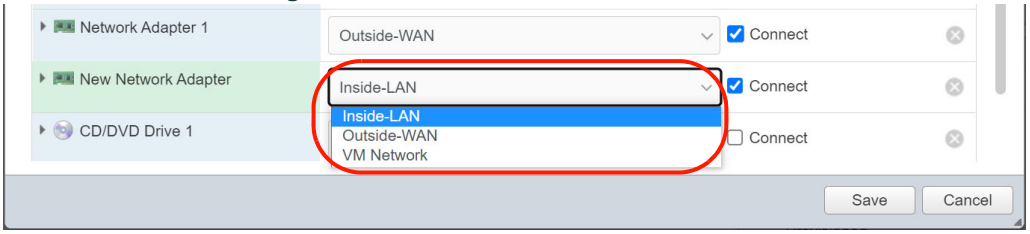


v. Click Save.

vi. Select Actions > Edit Settings again.

vii. In the Edit settings window, click Add network adapter.

viii. In the New Network Adapter list, select the adapter to use for the inside interface (eth1), which is the LAN (internal/local)-facing network.



ix. Click Save.

n. Configure ACM.

Deploying ACM VM From Live-CD (ISO) File

Note: ▪ *For detailed information about VMWare ESXi 7.0+, refer to documentation provided by VMWare.*
▪ *This procedure applies to both FIPS and non-FIPS deployments.*

To deploy an ACM VM on the ESXi 7.0+ server, using a Live-CD (.iso) file:

1. Get the ACM Live-CD ISO file. (Contact your Sierra Wireless Support representative for instructions on obtaining the file.)
2. On a Windows or Mac computer (Linux is not supported), open a browser and then connect to the vSphere Hypervisor client's IP address (for example, https://10.10.10.10). The vSphere Hypervisor client will appear.

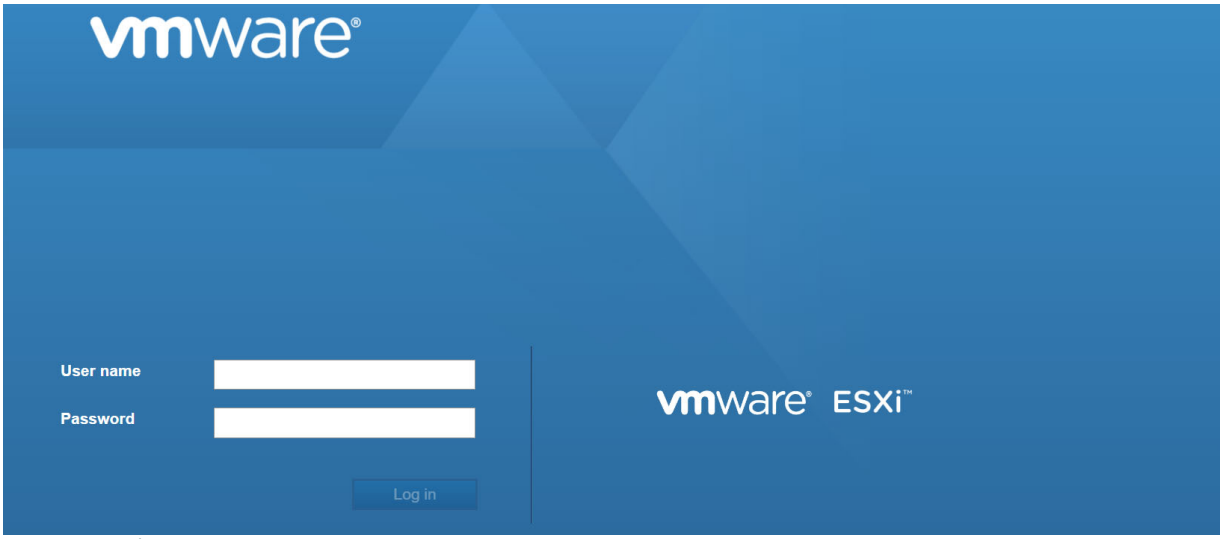


Figure 2-3: vSphere Hypervisor Login Screen

3. Enter the vSphere Hypervisor User name and Password, and click Log in.
   The vSphere Hypervisor interface appears.

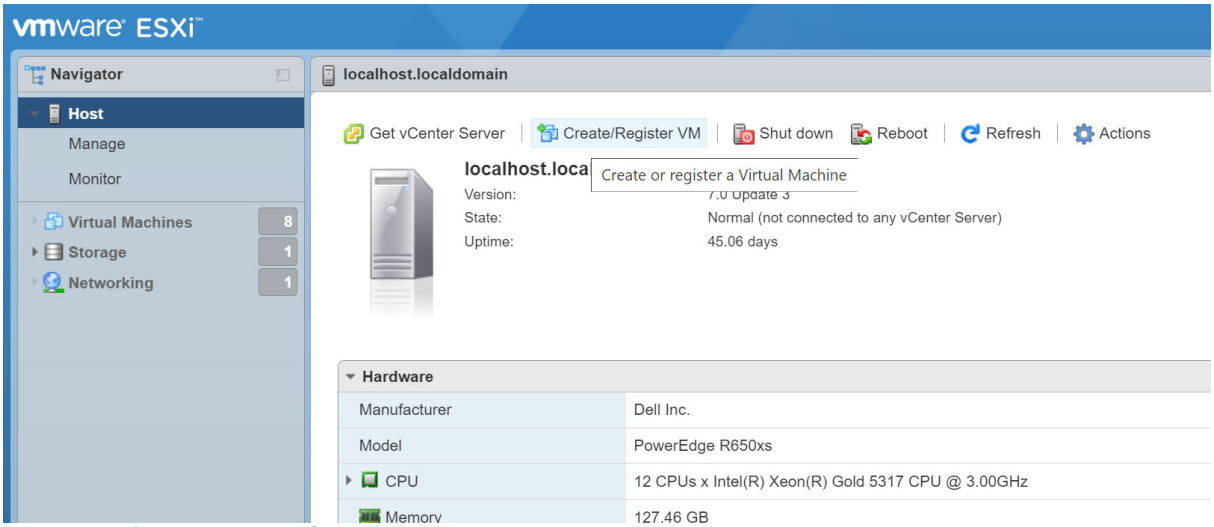
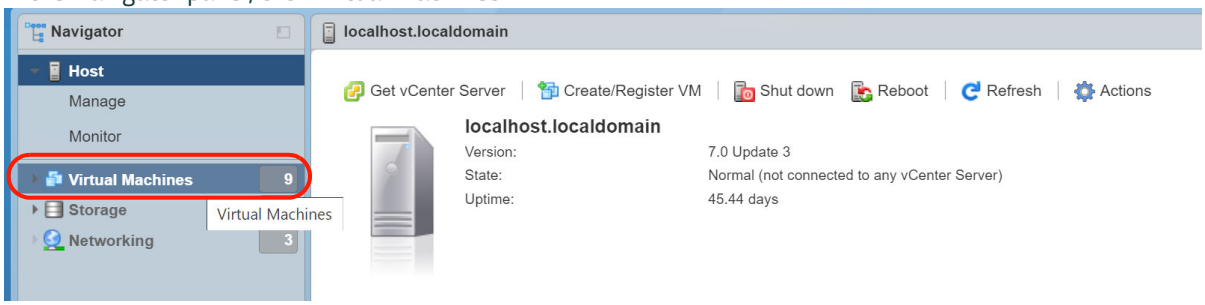


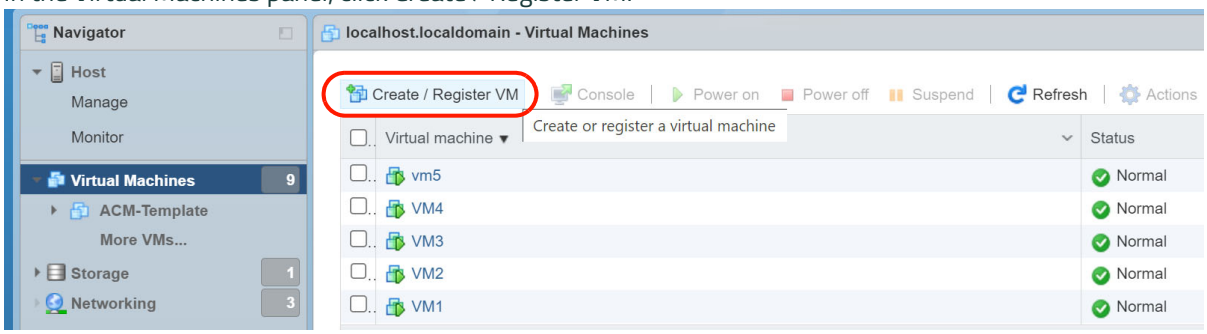
Figure 2-4: vSphere Hypervisor Interface

4. Create a VM:

   a. In the Navigator panel, click Virtual Machines.

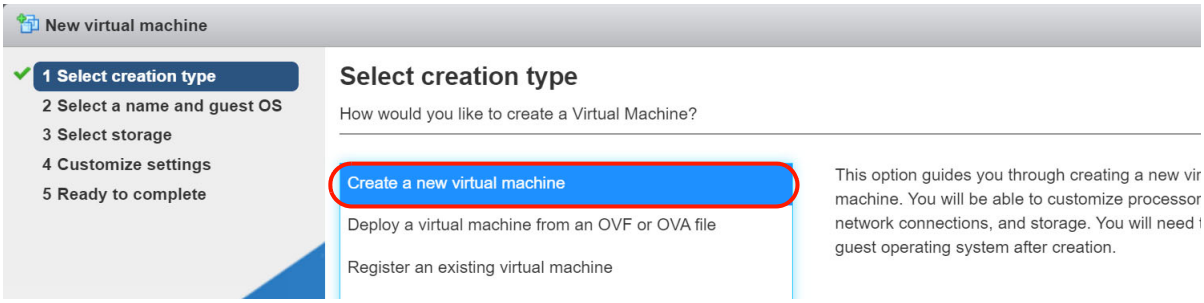


   b. In the Virtual Machines panel, click Create / Register VM.



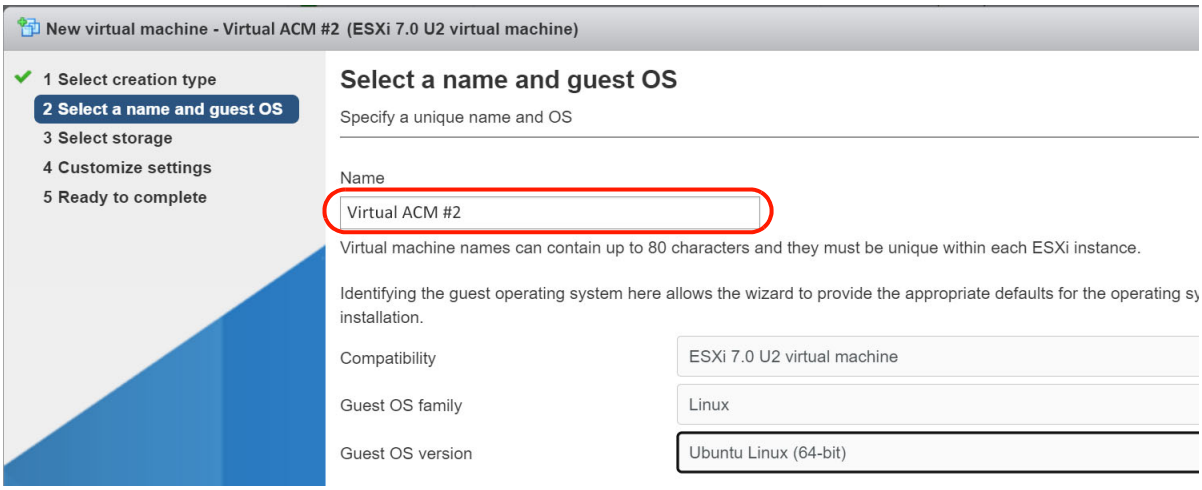
   The New Virtual Machine wizard appears.

c. In the Select creation type panel, select Create a new virtual machine.



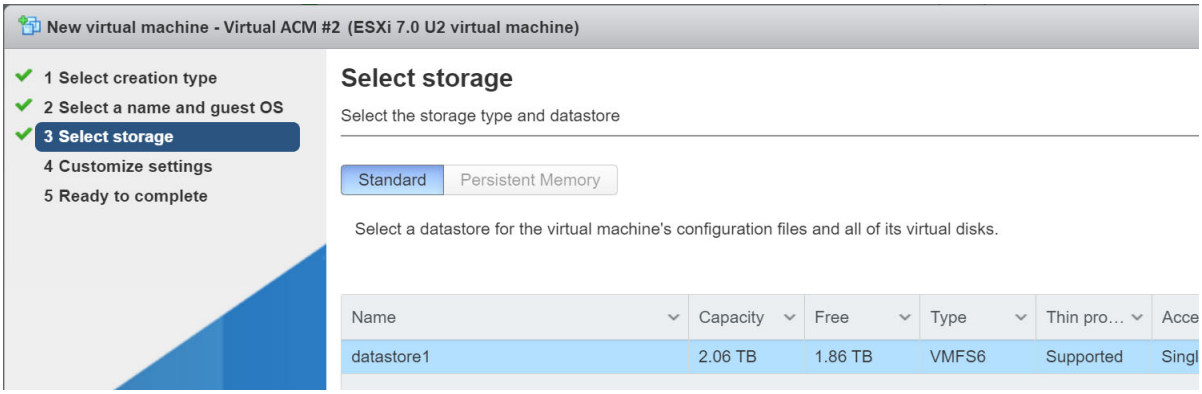
d. Click Next.

e. In the Select a name and guest OS panel, enter a unique name to identify the virtual machine (e.g., "Virtual ACM #2").

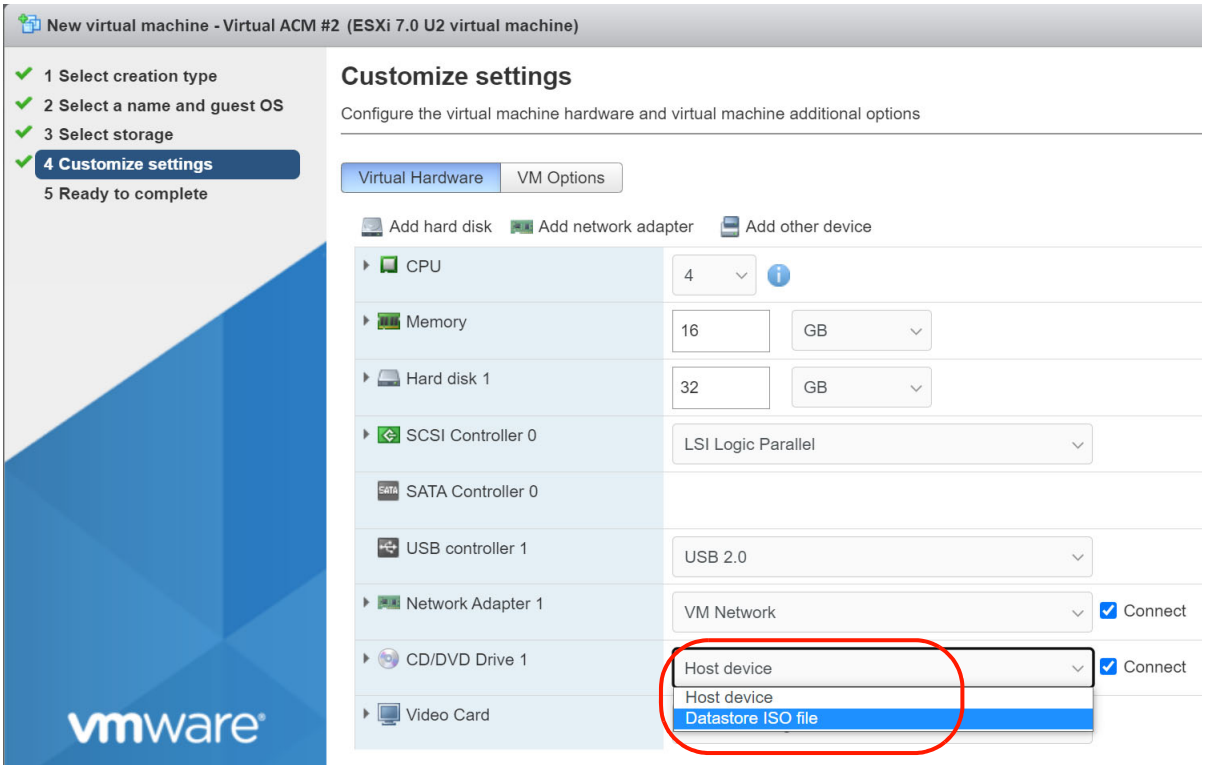


f. Click Next.

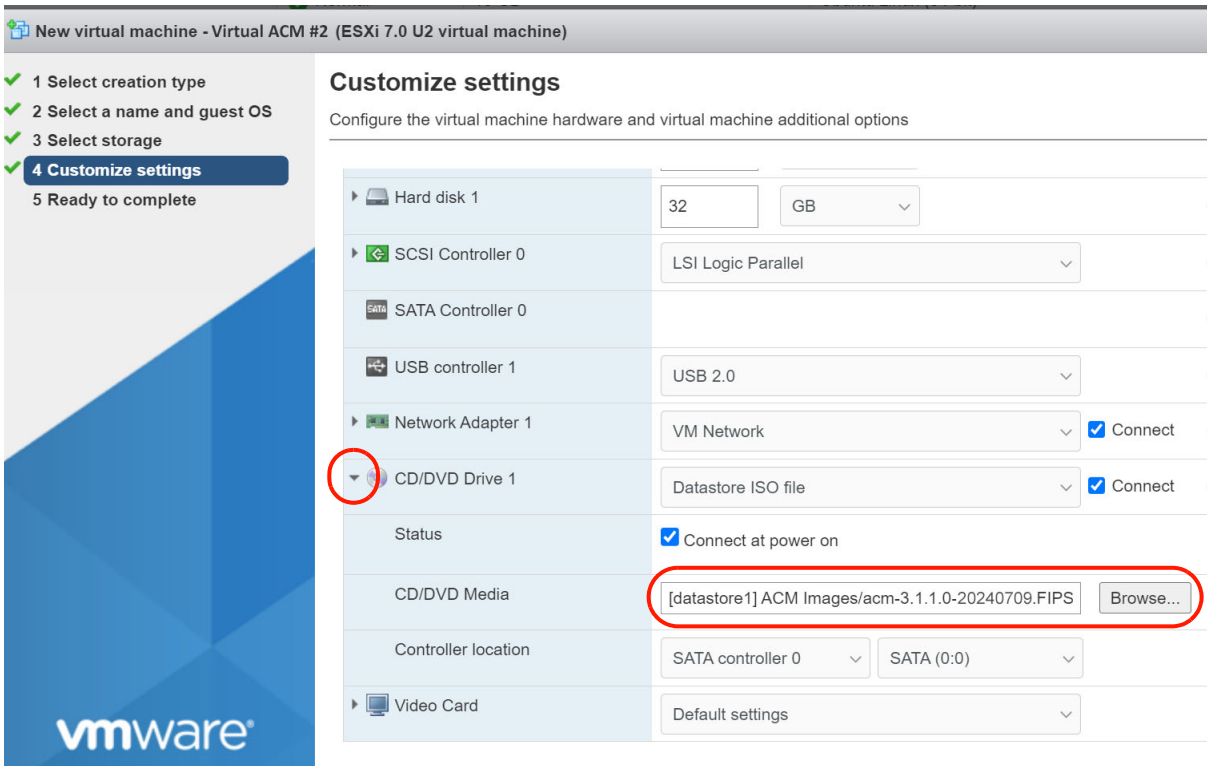
g. In the Select storage panel, no changes are needed. Click Next.



h. In the Customize settings panel, select Datastore ISO file from the CD/DVD Drive 1 picklist.

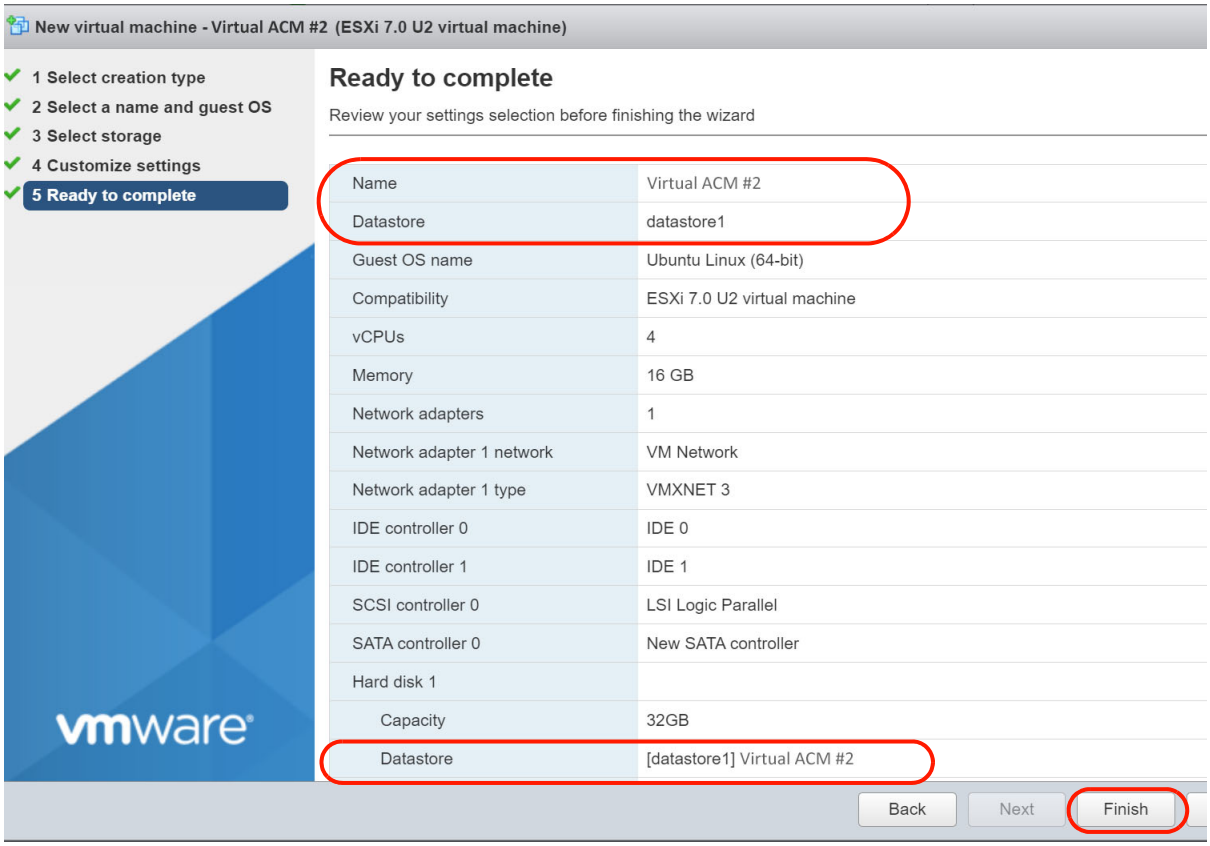


i. Expand the CD/DVD Drive 1 section and in the CD/DVD Media field, click Browse... to select your ACM Live-CD ISO file.



j. Click Next.

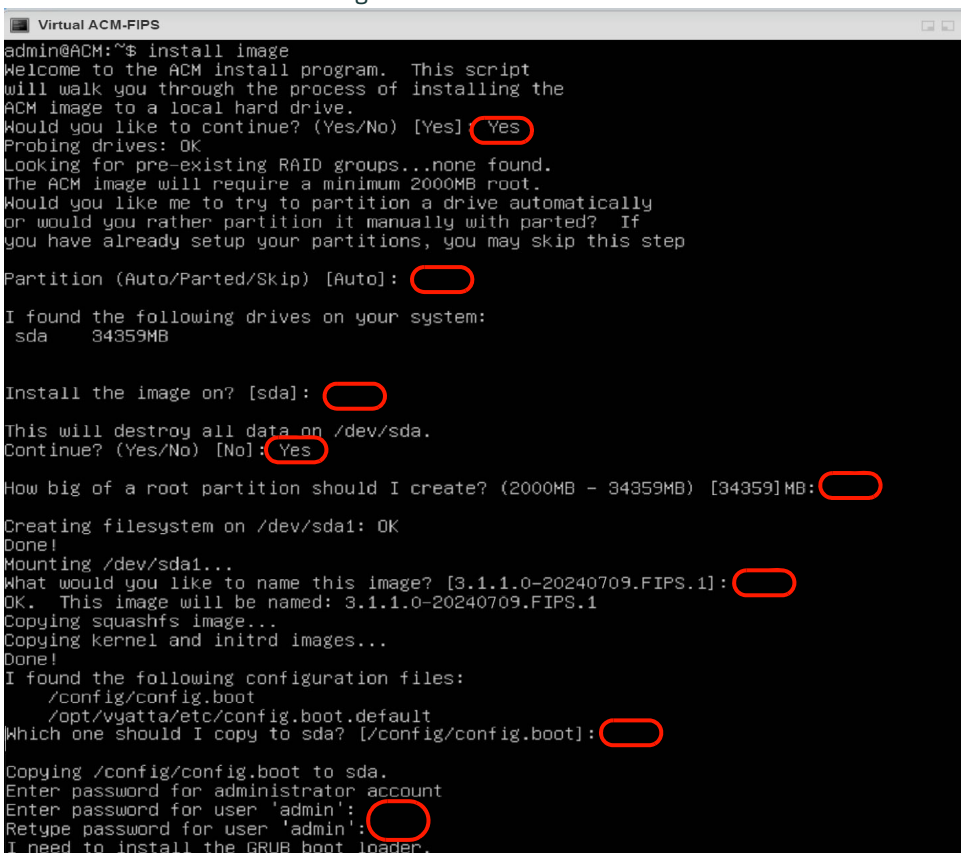
k. Review your options in the Ready to Complete panel and click Finish to deploy the virtual machine.



l. Reboot the new VM (in this example, Virtual ACM #2).

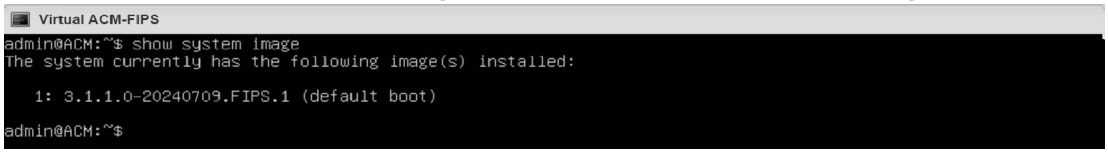
m. Enter the command "show system image" to confirm that the ACM is running from the Live-CD:

n. Enter the command “install image” to install the VM on the hard drive:



o. Reboot the new VM.

p. Enter the command “show system image” to confirm that the ACM is now running from the hard drive.



q. Configure ACM

Connecting ACM to Your Network

ACM is dedicated to providing secure mobile connections for AirLink routers. It is not to be used as a replacement or substitute general purpose enterprise firewall/router.

Sierra Wireless recommends that ACM be installed behind the enterprise firewall so that policies and procedures relating to enterprise security are not significantly affected by the introduction of ACM. When used in this mode, the ACM security footprint is limited as follows:

- AirLink devices must be able to access ACM from the WAN. Typically, this requires that ACM be assigned a public IP address. If the IP address is not publicly routable, it should be network address translated (NAT) (see next point) to a private address on the ACM physical network interface.
- TCP/IP port 2222 must be enabled to allow access to ACM.
- The traffic between AirLink devices and ACM consists of IPsec traffic on UDP protocol port 500 and ESP encapsulated on UDP port 4500. Only these items need to be taken into consideration for port and protocol translation from the public to the private address.

To connect ACM to your network, the following steps must be performed:

1. Assign a public IP address. If network address translation is required, translate assigned IP addresses to the outside address of the ACM (see Table A-1 on page 61).
2. At a minimum, enable the following protocols and ports for the translated address:
   - TCP/IP Port 2222
   - UDP/IP 500
   - UDP/IP 4500

If required by a customer security policy, the VPN between the AirLink router and the ACM can be specified to route ALL traffic through the secure connection. While there are some consequences with this approach, it does provide the advantage of lock down so that all content is delivered to the enterprise security environment where additional equipment can provide deep-packet inspection, anti-virus, and content filtering among other security services.

Connecting to ACM from an Inside Device

ACM is pre-configured with an inside network address and other information as specified in Important ACM Configuration Requirements on page 61.

1. Establish a 10/100/1000 Mbps Ethernet connection between the inside interface on Ethernet Port 2 of the ACM appliance and either an Ethernet switch or a direct connection on a PC.

   The default address and netmask of the Inside interface is 10.99.0.1/255.255.255.0.
2. Use an SSH client tool (such as putty.exe) running on a test PC to open an SSH session to port 2222 to the inside address.

Note: Sierra Wireless can only provide remote technical support for ACM if access to Port 2222 is enabled on the public or private interface. If only private interface access is available, an independent VPN access method must be provided.

3: Configuration Overview

This chapter describes some common tasks performed by the ACM Administrator.

Logging In and Out

To log in to ACM, use the default username (*admin*) and password (*inmotion*) as shown below (note — the welcome message will vary between distributions):

```
login as: admin
UNAUTHORIZED USE OF THIS SYSTEM IS PROHIBITED!
password: inmotion      ← Note: Password does not appear when typed.
   WELCOME TO ACM!
   This system is open-source software.
   The exact distribution terms for each module
   comprising the full system are described in the
   individual files in /usr/share/doc/*/copyright.
   Last login: Fri Apr 20 11:29:35 2016 from
   xyz.com

admin@ACM:~$
```

Important: *Sierra Wireless strongly recommends that you immediately change the Admin password from the default value ("inmotion") to prevent unauthorized use of the system. See Admin Password on page 34 for details.*

To log out of ACM, use the *exit* command:

```
admin@ACM:~$ exit
```

Change to Configuration Mode

By default, the system will be in operational mode after logging in to ACM, as indicated by the ":~$" prompt.

To modify the ACM configuration, the system must first be changed to configuration mode. To change to configuration mode, enter the *configure* command:

```
admin@ACM:~$ configure
```

The prompt for configuration mode will change to "#" as shown here:

```
admin@ACM#
```

Note: To change back to operational mode from configuration mode, use the "exit" command.

Configuration Tree

The ACM configuration is stored in attributes and nodes:

- Attribute — Includes a name and a data value.
- Node — A container for one or more attributes. A node can also contain sub-nodes to form a hierarchy of nodes.

Attributes and nodes are referred to as 'statements' when they are viewed from the command line using the 'show' command.

The following snippet (from 'show config' output) is an example of an attribute, node, and subnode:

```
local-ip 192.168.12.242   ← Attribute (name = 'local-ip',
                              value = IP address 192.168.12.242)
tunnel 1 {                ← Node
   esp-group 1            ← Attribute (name = 'esp-group',
                              value = 1)
   local {                ← Sub-node
      subnet 0.0.0.0/0    ← Attribute (name = 'subnet',
                              value = 0.0.0.0/0)
   }
}
```

Note: Nodes always have an enclosing pair of { } braces.

Manage Configuration Attributes

When the ACM appliance boots, its *boot configuration* is loaded into its *running configuration*. While the appliance is running, configuration attributes are managed using the commands shown in Table 3-1.

Table 3-1: Configuration Attribute Management Commands

Command	Purpose	Details
set	Add or modify an attribute.	See Add or Modify Attributes on page 27.
del **delete**	Delete an attribute.	See Delete Attributes on page 28.
sh **show**	Display all pending attribute changes (add, modify, delete).	See Show Uncommitted Attribute Changes on page 28.
discard	Remove all pending attribute changes.	See Discard Uncommitted Attribute Changes on page 29.
commit	Apply all pending attribute changes to the currently running configuration.	See Apply Configuration on page 29
save	Save the running configuration as the boot configuration.	See Save Configuration on page 30
load	Load the ACM's default configuration attributes.	See Restore Default Configuration on page 30

Note: Attribute changes (adding, modifying, deleting, loading defaults) do not take effect on ACM until they are first committed to the running configuration. After committing the changes, they stay in effect until the appliance reboots. To keep them in effect across reboots, they must be saved before the appliance reboots.

Add or Modify Attributes

To add a new attribute statement or modify an existing statement, use the *set* command.

The following example demonstrates the *set* command being used to make the following changes, and a snippet from the *show* command which displays the '+' and '>' symbols:

- Change the hash method for an esp group's "proposal 1" from "sha1" to "sha2_256"
- Add a new "proposal 2" to the esp group
- Add the encryption method for the new "proposal 2"

```
user@ACM1-Production# set vpn ipsec esp-group espgroup1 proposal 1 hash sha2_256
user@ACM1-Production# set vpn ipsec esp-group espgroup1 proposal 2 encryption aes256
user@ACM1-Production# show
...
esp-group espgroup1 {
    compression enable
    mode tunnel
    pfs enable
    proposal 1 {
        encryption aes256
        hash sha2_256
    }
+   proposal 2 {
+       encryption aes256
+   }
}
```

Delete Attributes

To delete an attribute statement, use the *delete* command.

The following example demonstrates the *delete* command being used to make the following change, and a snippet from the *show* command that displays the '-' symbol:

- Delete the hash method for an esp group's "proposal 1"

```
user@ACM1-Production# delete vpn ipsec esp-group espgroup1 proposal 1 hash
user@ACM1-Production# show
...
esp-group espgroup1 {
    compression enable
    mode tunnel
    pfs enable
    proposal 1 {
        encryption aes256
-       hash md5
    }
}
....
```

Show Uncommitted Attribute Changes

To view pending attribute changes, use the *show* command.

When the command is used:

- The plus (+) symbol appears next to new attributes
- The greater than (>) symbol appears next to modified attributes
- The minus (-) symbol appears next to deleted attributes

The following example demonstrates a snippet from the *show* command which displays:

- '>' for an encryption method being modified
- '–' for a hash method being deleted
- '+' for a proposal being added

```
user@ACM1-Production# show
...
esp-group espgroup1 {
    compression enable
    mode tunnel
    pfs enable
    proposal 1 {
>       encryption aes256
-       hash md5
    }
+   proposal 2 {
+       encryption aes256
+   }
}
....
```

Discard Uncommitted Attribute Changes

To remove pending attribute changes so they cannot be committed to the running configuration, use the *discard* command.

After discarding the configuration changes, the configuration reverts to the state it was in prior to the changes and the symbol(s) (+, -, or >) located beside the changed attribute statement(s) disappear.

The following example shows the *discard* command being used and a snippet from the *show* command which displays:

- The original attribute values for proposal 1
- No proposal 2 (it is no longer being added)

```
user@ACM1-Production# discard

  Changes have been discarded

user@ACM1-Production# show
...
esp-group espgroup1 {
    compression enable
    mode tunnel
    pfs enable
    proposal 1 {
       encryption aes128
       hash md5
    }
}
....
```

Apply Configuration

To apply changes to the ACM configuration, use the *commit* command.

After applying the configuration changes, the symbol(s) (+, -, or >) located beside the changed attribute statement(s) disappear as shown in the example below.

Note: Committing applies the changes only to the currently running configuration. For the committed changes to remain active after rebooting, they must be saved to the boot configuration as described in *Save Configuration on page 30.*

The following example shows the *commit* command being used when there pending changes, and a snippet from the *show* command which shows that all changes have been applied (there are no '+', '>', or '–' symbols):

```
admin@ACM# commit
user@ACM1-Production# show
...
esp-group espgroup1 {
    compression enable
    mode tunnel
    pfs enable
    proposal 1 {
        encryption aes256    ← changed from aes128
    }                        ← hash attribute was deleted
    proposal 2 {             ← proposal 2 was added
        encryption aes256
    }
}
....
```

Save Configuration

Use the *save* command to save committed changes to the boot configuration so that they remain active across reboots.

```
admin@ACM# save
```

Restore Default Configuration

You can restore ACM to its default configuration using the *load*, *commit*, and *save* commands in configuration mode, as shown below.

Warning: *This process COMPLETELY replaces ACM's current configuration, so should be used only when absolutely necessary. DO NOT perform this via a remote login session — if you do, you will lose your connection to ACM when the configuration (including the outside IP address) is replaced.*

```
admin@ACM:~# load /opt/vyatta/etc/config.boot.default
admin@ACM:~# commit    ← Commits changes to running configuration
admin@ACM:~# save      ← Saves changes as boot configuration
```

Remote Logging (Syslog) Setup

ACM can be configured to support remote logging as a client of an external Syslog server so all ACM system logs will be forwarded to the external server.

1. First, configure the external Syslog server — Configure External Syslog Server.
2. Then configure ACM as a client — Configure ACM Server as Syslog Client.

   When ACM has been properly configured as a client, the external Syslog server receives all log messages from ACM — Verify External Syslog Server Behavior.

Configure External Syslog Server

Important: *The following is an example Ubuntu-based external server configuration to be used as a general guide; the specific configuration steps may vary depending on the Ubuntu version being used. Refer to your Ubuntu documentation for specific configuration details.*

Note: In this example, the Linux Ubuntu Desktop (VM) is acting as the external Syslog server with IP address 10.203.76.56.

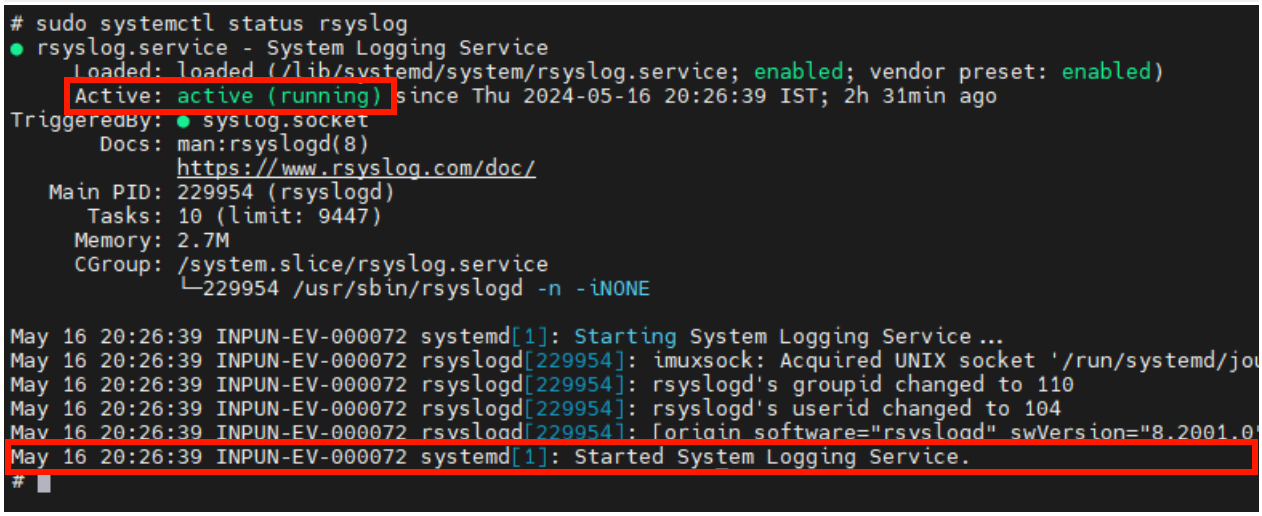
To configure the Linux Ubuntu Desktop (VM) to act as a Syslog server:

1. Log in to the Linux Ubuntu Desktop (VM).
2. Elevate your user priveleges:
```
# sudo su
```
3. Edit /etc/rsyslog.conf (the message logging service configuration file):
   - Make sure the 'imudp' and 'imtcp' lines are uncommented:
```
# /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf
#################
#### MODULES ####
#################
module(load="imuxsock") # provides support for local system logging
#module(load="immark")  # provides --MARK-- message capability
# provides UDP syslog reception
module(load="imudp") ← Uncomment this line
input(type="imudp" port="514") ← Uncomment this line
# provides TCP syslog reception
module(load="imtcp") ← Uncomment this line
input(type="imtcp" port="514") ← Uncomment this line
```
   - Add the two 'RemInputLogs' lines below the 'imtcp' section:
```
# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514")

$template RemInputLogs, "/var/log/remotelogs/%FROMHOST-IP%/syslog.log" ← Add this line
*.* ?RemInputLogs ← Add this line
```
4. Save the configuration file.
5. Restart the rsyslog service:
```
# sudo systemctl restart rsyslog
```

6. Confirm that the rsyslog service is active (running):

```
# sudo systemctl status rsyslog
```



Configure ACM Server as Syslog Client

To configure the ACM Syslog service as a client of an external Syslog server, log in to ACM and go to configuration mode, then:

1. Configure ACM and the log level to forward the ACM syslog to an external server:

```
admin@ACM:~$ set system syslog host <SyslogServer_IPv4_address> facility all level all
```

where:

- <SyslogServer_IPv4_address> — The external server's address (e.g., 10.203.76.56)
- "facility all" — Logs from all systems (except 'mark') will be forwarded to the external server.
- "level all" — All logs (any severity) will be forwarded to the external server.

2. Confirm the configuration matches the example below:

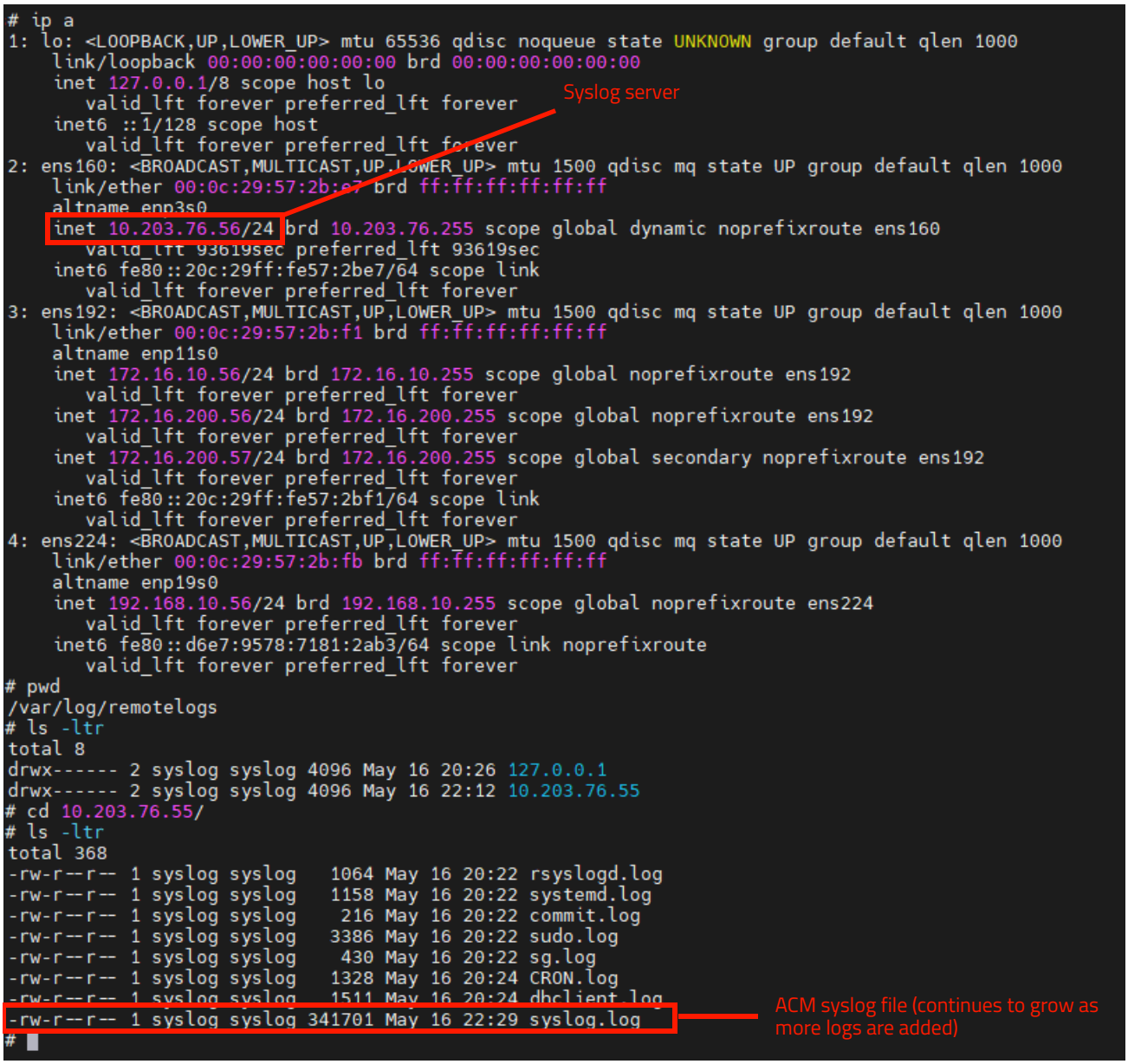
```
admin@ACM:~$ show system syslog
global {
    facility all {
        level warning
    }
    facility daemon {
        level debug
    }
}
host <SyslogServer_IPv4_address> {
    facility all {
        level all
    }
}
```

Verify External Syslog Server Behavior

After the external Syslog server has been properly configured and is running, all log messages from configured clients (e.g., ACM) will be placed on the server under the folder /var/log/remotelogs in folders using the client's IP address:

- Syslog folder: /var/log/remotelogs
- Client folder: /var/log/remotelogs/<ACM_IPv4_address> (e.g., 10.203.76.55)
- Client's Syslog file: /var/log/remotelogs/<ACM_IPv4_address>/syslog.log

For example:




```
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:57:2b:e7 brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 10.203.76.56/24 brd 10.203.76.255 scope global dynamic noprefixroute ens160
       valid_lft 93619sec preferred_lft 93619sec
    inet6 fe80::20c:29ff:fe57:2be7/64 scope link
       valid_lft forever preferred_lft forever
3: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:57:2b:f1 brd ff:ff:ff:ff:ff:ff
    altname enp11s0
    inet 172.16.10.56/24 brd 172.16.10.255 scope global noprefixroute ens192
       valid_lft forever preferred_lft forever
    inet 172.16.200.56/24 brd 172.16.200.255 scope global noprefixroute ens192
       valid_lft forever preferred_lft forever
    inet 172.16.200.57/24 brd 172.16.200.255 scope global secondary noprefixroute ens192
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe57:2bf1/64 scope link
       valid_lft forever preferred_lft forever
4: ens224: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:0c:29:57:2b:fb brd ff:ff:ff:ff:ff:ff
    altname enp19s0
    inet 192.168.10.56/24 brd 192.168.10.255 scope global noprefixroute ens224
       valid_lft forever preferred_lft forever
    inet6 fe80::d6e7:9578:7181:2ab3/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
# pwd
/var/log/remotelogs
# ls -ltr
total 8
drwx------ 2 syslog syslog 4096 May 16 20:26 127.0.0.1
drwx------ 2 syslog syslog 4096 May 16 22:12 10.203.76.55
# cd 10.203.76.55/
# ls -ltr
total 368
-rw-r--r-- 1 syslog syslog   1064 May 16 20:22 rsyslogd.log
-rw-r--r-- 1 syslog syslog   1158 May 16 20:22 systemd.log
-rw-r--r-- 1 syslog syslog    216 May 16 20:22 commit.log
-rw-r--r-- 1 syslog syslog   3386 May 16 20:22 sudo.log
-rw-r--r-- 1 syslog syslog    430 May 16 20:22 sg.log
-rw-r--r-- 1 syslog syslog   1328 May 16 20:24 CRON.log
-rw-r--r-- 1 syslog syslog   1511 May 16 20:24 dhclient.log
-rw-r--r-- 1 syslog syslog 341701 May 16 22:29 syslog.log
#
```

For a deeper explanation of how to set up remote logging, see www.thegeekstuff.com/2012/01/rsyslog-remote-logging/ and //www.linkedin.com/pulse/how-install-set-up-rsyslog-server-linux-ubuntu-20041-akshay-sharma/.

4: Networking / Routing Configuration

Admin Password

Important: *Sierra Wireless strongly recommends that you immediately change the Admin password from the default value to prevent unauthorized use of the system.*

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.

Host Name

To change ACM's default hostname, use the following commands:

```
admin@ACM:~# set system host-name <HOST-NAME>
admin@ACM:~# commit
```

Domain Name

To change ACM's domain name, use the following commands:

```
admin@ACM:~# set system domain-name <DOMAIN-NAME>
admin@ACM:~# commit
```

OUTSIDE Interface IP Address

To change the IP address of the OUTSIDE interface, use the following commands:

```
admin@ACM:~# set interfaces ethernet eth0 address <WAN-IP-ADDRESS/SUBNET-BITMASK>
admin@ACM:~# commit
```

Default Gateway

To change the default gateway, use the following commands:

```
admin@ACM:~# set system gateway-address <DEFAULT-GATEWAY-IP-ADDRESS>
admin@ACM:~# commit
```

INSIDE Interface IP Address

To change the IP address of the INSIDE interface, use the following commands.

Note: The default IP address must also be deleted as shown below.

```
admin@ACM:~# delete interfaces ethernet eth1 address 10.99.0.1/24
admin@ACM:~# set interfaces ethernet eth1 address <LAN-IP-ADDRESS/SUBNET-BITMASK>
admin@ACM:~# commit
```

INSIDE Routing Information IP Address

To specify how VPN traffic will be routed from ACM to the enterprise network application servers (only if intermediate routers exist) use the following command:

```
admin@ACM:~# set protocols static route <ENTERPRISE-NETWORK/MASK> next-hop <NEXT-HOP-IP-ADDRESS>
```

DNS Server

To change the DNS server, use the following commands:

```
admin@ACM:~# set system name-server <DNS-IP-ADDRESS>
admin@ACM:~# commit
```

5: VPN Configuration

Server-side (ACM) VPN Configuration

IPsec VPN

ACM uses the strongSwan internet protocol security (IPsec) implementation for securing communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

The following parameters must be defined to be able to configure an IPsec VPN:

- Phase 1 and Phase 2 negotiation parameters:
  - Encryption
  - Hashing
  - Key exchange method
- IDs for each side — IP address for ACM, <PeerID> for the peer
- Source and destination IP address of the protected traffic
- Pre-shared secret or certificate

ACM stores Phase 1 and Phase 2 parameters in groups (IKE for phase 1, and ESP for phase 2) that can be reused in multiple VPN configurations.

ACM IKE / ESP Negotiation Parameters

Supported IKE (Phase 1) / ESP (Phase 2) negotiation parameters for ACM 3.1.1 (non-FIPS) and ACM 3.1.1 (FIPS) are listed in Table 5-1.

Table 5-1: ACM IKE / ESP Parameter Support

Type	ACM 3.1.1 (non-FIPS)		ACM 3.1.1 (FIPS)	
	IKE	ESP	IKE	ESP
Encryption				
aes128	Y	Y	Y	Y
aes128ccm16	—	—	—	Y[a]
aes128gcm16	Y[a]	Y[a]	Y[a]	Y[a]
aes192	Y	Y	Y	Y
aes192gcm16	Y	Y	Y	Y
aes256	Y	Y	Y	Y
aes256ccm16	—	—	—	Y[a]
aes256gcm16	Y[a]	Y[a]	Y[a]	Y[a]
3des	Y[b]	Y[b]	—	—

Table 5-1: ACM IKE / ESP Parameter Support (Continued)

Type	ACM 3.1.1 (non-FIPS)		ACM 3.1.1 (FIPS)	
	IKE	ESP	IKE	ESP
Hash				
sha1	Y[b]	Y[b]	—	—
sha2_256	Y	Y	Y	Y
sha2_384	Y	Y	Y	Y
sha2_512	Y	Y	Y	Y
md5	Y[b]	Y[b]	—	—
none	—	—	—	Y[a]
DH Group				
1	—	—	—	—
2	Y[b]	Y[b]	—	—
5	Y[b]	Y[b]	—	—
14	Y	Y	Y	Y
15	Y	Y	Y	Y
16	Y	Y	Y	Y
17	Y	Y	Y	Y
18	Y	Y	Y	Y
19	Y	Y	Y	Y
20	Y	Y	Y	Y
21	Y	Y	Y	Y
26	Y	Y	Y	Y
none	—	Y[c]	—	—

a. When aes128ccm16, aes128gcm16, aes256ccm16, or aes256gcm16 encryption is used, hash must be none.
b. Indicated cryptographic protocols are less secure than other options and are not recommended.
c. DH group 'none' is not recommended. For greater security, choose a supported ESP DH group.

IKE Group Configuration

The procedure for configuring IKE groups varies depending on the IKE version being used.

Important: *IKEv2 is supported and should be used on:*

- *AirLink oMG2000/500 and MG90 routers*
- *AirLink XR80/XR90 routers*
- *Other AirLink devices running ALEOS 4.12.0 or later*
- *NCP Client for Windows*

Note that AirLink devices running older ALEOS versions (pre-ALEOS 4.12.0) support only IKEv1.

To configure IKE groups with:

- IKEv2 — See Configure IKE Groups with MOBIKE (IKEv2) on page 38.
- IKEv1 — See Configure IKE Groups with IKEv1 on page 39.

Configure IKE Groups with MOBIKE (IKEv2)

Note: IKEv2 is now supported on AirLink devices running ALEOS 4.12.0 or later and should be used for those devices. To configure IKE groups for devices running older ALEOS versions (i.e., pre-ALEOS 4.12.0), see Configure IKE Groups with IKEv1 on page 39.

When used on supported devices, the MOBIKE (IKEv2 Mobility and Multihoming) protocol allows for fast, seamless VPN tunnel switching. Combining the AirLink routers' intelligent WAN management with MOBIKE ensures the delivery of secure and extremely high performance mobile communications.

To enable this switching feature, both ACM and the peer (supported device) must:

- Enable IKEv2 as the Key Exchange Mechanism
- Enable MOBIKE

Use the *set vpn ipsec ike-group* command to configure the IKE group parameters, as described below.

Note: The attribute values used in the commands below are examples only; use values that are appropriate for your configuration. Valid values for some IKE group configurations are described in Table 5-1 on page 36.

1. Configure the IKE group(s) — There can be more than one IKE group and they can be called independently for different peers. The IKE group name can be any string.

```
set vpn ipsec ike-group <IKE-GRP-NAME>
```

2. After configuring your IKE group(s), configure Dead Peer Detection (DPD):
   a. For each group, enable DPD:

```
set vpn ipsec ike-group <IKE-GRP-NAME> dead-peer-detection action clear
```

   Important: *Always enable DPD, and always use "action clear" — do NOT use "action hold" or "action restart".*

   b. After enabling DPD on the IKE group(s), set the global DPD parameters (these apply to DPD for all groups) — If not specified, default values are used (30 second timeout, 3 retries):

```
set vpn ipsec ikev2-retransmit-timeout 15
set vpn ipsec ikev2-retransmit-tries 1
```

Note: Do not use the IKEv1 DPD configuration options "dead-peer-detection interval" and "dead-peer detection timeout"—these are not supported in IKEv2.

3. Configure IKE Version and MOBIKE:

```
set vpn ipsec ike-group <IKE-GRP-NAME> ike-version ikev2
set vpn ipsec ike-group <IKE-GRP-NAME> mobike yes
```

4. Configure IKE transform set proposals (Note: There can be more than one proposal.) See Table 5-1 on page 36 for supported parameter values:

```
set vpn ipsec ike-group <IKE-GRP-NAME> proposal 10 dh-group <Dh_group_type>
set vpn ipsec ike-group <IKE-GRP-NAME> proposal 10 encryption <Encrypt_type>
set vpn ipsec ike-group <IKE-GRP-NAME> proposal 10 hash <Hash_type>
```

Configure IKE Groups with IKEv1

Note: IKEv2 should be used for AirLink oMG2000/500 and MG90 routers, XR series routers, and other AirLink devices running ALEOS 4.12.0 or later—see Configure IKE Groups with MOBIKE (IKEv2) on page 38 to configure IKE groups for those devices.

The following AirLink routers support only the IKEv1 protocol (IKEv2 is not supported):

- RV and MP series running pre-ALEOS 4.12.0
- ES, GX series

Use the *set vpn ipsec ike-group* command to configure the IKE group parameters, as described below.

Note: The attribute values used in the commands below are examples only; set the values as appropriate for your configuration.

1. Configure the IKE group(s)—There can be more than one IKE group and they can be called independently for different peers. The IKE group name can be any string.

```
set vpn ipsec ike-group <IKE-GRP-NAME>
```

2. After configuring your IKE group(s), configure Dead Peer Detection (DPD) for each group:
   a. Enable DPD:

```
set vpn ipsec ike-group <IKE-GRP-NAME> dead-peer-detection action clear
```

   Important: *Always enable DPD, and always use "action clear"—do NOT use "action hold" or "action restart".*

   b. Set the DPD parameters (these must be set for each group):

```
set vpn ipsec ike-group <IKE-GRP-NAME> dead-peer-detection interval <Interval_seconds>
set vpn ipsec ike-group <IKE-GRP-NAME> dead-peer-detection timeout <Timeout_seconds>
```

Note: Do not use the IKEv2 DPD configuration options "ikev2-retransmit-timeout" and "ikev2-retransmit -tries"—these are not supported in IKEv1.

3. Configure the IKE version:
```
set vpn ipsec ike-group <IKE-GRP-NAME> ike-version ikev1
```
4. Configure IKE transform set proposals (Note: There can be more than one proposal.) See Table 5-1 on page 36 for supported parameter values:
```
set vpn ipsec ike-group <IKE-GRP-NAME> proposal 10 dh-group <Dh_group_type>
set vpn ipsec ike-group <IKE-GRP-NAME> proposal 10 encryption <Encrypt_type>
set vpn ipsec ike-group <IKE-GRP-NAME> proposal 10 hash <Hash_type>
```

ESP Group

Use the *set vpn ipsec esp-group* command to configure the ESP group parameters, as described below.

Note: The attribute values used in the commands below are examples only; set the values as appropriate for your configuration.

1. Configure the ESP Group(s) — There can be more than one ESP group and they can be called independently for different peers. The <ESP-GRP-NAME> can be any string.
```
set vpn ipsec esp-group <ESP-GRP-NAME>
```
2. After configuring your ESP Group(s), configure the following group parameters:
   - Compression option:
```
set vpn ipsec esp-group <ESP-GRP-NAME> compression disable
```

     Note: IP compression is supported only with devices running ALEOS 4.14 or later. IP compression must be disabled for devices running MGOS or AirLink OS.
     If IP compression is enabled, additional CPU resources will be used and VPN throughput will be reduced.
   - ESP mode:
```
set vpn ipsec esp-group <ESP-GRP-NAME> mode tunnel
```
   - ESP transform set proposals (Note: There can be more than one proposal.) See Table 5-1 on page 36 for supported parameter values:
```
set vpn ipsec esp-group <ESP-GRP-NAME> proposal 10 encryption <Encrypt_type>
set vpn ipsec esp-group <ESP-GRP-NAME> proposal 10 hash <Hash_type>
```
   - DH Group — The dh-group is required for AirLink routers (except oMG/MG90), optional for NCP client peers, and must not be used for oMG/MG90 routers. See Table 5-1 on page 36 for supported parameter values.
```
set vpn ipsec esp-group <ESP-GRP-NAME> proposal 10 dh-group <Dh_group_type>
```

Global Firewall Rules

ACM supports the use of a minimal number of global firewall rules to streamline VPN connection requests from deployed devices. One (or a few) global firewall rules can replace the per-VPN tunnel firewall rules for any deployment size (from small to very large).

By default, ACM uses strongSwan to automatically create per-VPN tunnel firewall rules allowing IPsec packets to pass from the WAN to the ACM LAN. In large deployments (several hundred or more devices) where many devices include multiple subnets, the time required for strongSwan to create the per-VPN rules can increase past the connection timeout periods of individual devices, causing those devices to drop their connection attempts.

With global firewall rules, IPsec-secured access is provided to large groups of devices in IP address subnets (to be obtained from the network engineer who sets up ACM), eliminating the processing requirement for setting up individual rules.

To use global firewall rules:

1. Obtain the subnet(s) to use from the network engineer configuring ACM. For example, the engineer could define:
   - Deployment of up to 512 devices — 172.16.31.0/24 and 172.18.1.0/24
   - Deployment of up to 2046 devices — 172.17.254.0/20
2. For each subnet, define the global firewall forwarding rules:

```
set firewall name DEFAULT_FWD rule <rule_num> action accept
set firewall name DEFAULT_FWD rule <rule_num> ipsec match-ipsec
set firewall name DEFAULT_FWD rule <rule_num> source address <subnet>
```

   For example (using the example 512-device subnets from step 1):

```
set firewall name DEFAULT_FWD rule 1 action accept
set firewall name DEFAULT_FWD rule 1 ipsec match-ipsec
set firewall name DEFAULT_FWD rule 1 source address 172.16.31.0/24
set firewall name DEFAULT_FWD rule 2 action accept
set firewall name DEFAULT_FWD rule 2 ipsec match-ipsec
set firewall name DEFAULT_FWD rule 2 source address 172.18.1.0/24
```

3. Make sure, when configuring individual VPN Peers, to set the auto-firewall option to 'no' (see instructions in next section).

VPN Peers

To provision tunnels for VPN peers (including supported AirLink routers, and NCP Client for Windows), ACM must be configured with the peers' IDs and other attributes.

Configure VPN Peer IDs

To configure a VPN peer ID on ACM, Use the following command:

```
set vpn ipsec site-to-site peer <PeerID>
```

where <PeerID> is one of the supported types described in Table 5-2 on page 42, or "any".

If the <PeerID> is:

- A supported Peer ID Type from Table 5-2 — ACM creates connections for each peer, using different PSKs. This is the preferred method for oMG/MG90 routers and other AirLink routers, as it allows both the router and the client devices of the router to use the VPN tunnels.
- "any" — ACM creates Host2LAN connections with peers of the same type (AirLink routers, NCP clients) without having to specify their IDs individually. All the peers will share the same pre-shared key (PSK).
  This method is suitable for NCP clients since NCP operates on a host device (laptop) and has no client devices that would require VPN access.
  This method is not recommended for AirLink routers, as only the router can use the VPN tunnel — its client devices cannot.

Table 5-2: VPN Peer ID Types

Peer	Location in Software	Peer ID Types
Note: Make sure to use the described formats to enter peer IDs in the peer's software interface, and use the same formats when entering the IDs on the ACM in the "set vpn ipsec site-to-site peer" command.		
oMG/MG90	WAN > VPNs > (Edit or Add) Field: Auth ID	Recommended type: ▪ ESN — Router's unique serial number (<ESN>) Format: @<ESN> Alternate types ▪ ip address Format: <IP> ▪ custom: Format: @<custom>
AirLink ES, GX, LX, MP, RV series	VPN > VPN# Field: Peer Identity Type	Recommended type: ▪ FQDN — Free-format string. User must ensure this is a unique string. Format: @<FQDN> Alternate types: ▪ User FQDN — Free-format string. User must ensure string is unique. Format: @@<USER_FQDN> ▪ IP — Router's IP address Format: <IP> *Note: If FQDN or User FQDN is used, read Main/Aggressive Mode Configuration on page 49 for additional instructions.*
AirLink RX55, XR80/XR90	Networking > VPN > IPsec Tunnels > CREATE IPSEC TUNNEL Field: PEERS	Required type: ▪ IP address — Router's IP address Format: <IP>
NCP Client for Windows	Profiles > Identities Field: Type	Recommended type: ▪ Fully Qualified Domain Name Format: @<FQDN> Alternate types: ▪ IP Address Format: <IP> ▪ Fully Qualified Username Format: @@<User_FQDN> ▪ ASN1 Distinguished Name Format: <ASN1 Dname> (Note: Required if using certificate authentication.) Not compatible with ACM: ▪ IP Subnet Address ▪ ASN1 Group Name ▪ Free string

Configure VPN Peer Attributes

For each VPN peer, configure the following attributes:

Note: In these commands, replace <PeerID> with the peer ID type used by ACM (described in Configure VPN Peer IDs on page 41.

- PSK for the peer:

```
set vpn ipsec site-to-site peer <PeerID> authentication mode pre-shared-secret
set vpn ipsec site-to-site peer <PeerID> authentication pre-shared-secret <PRESHARED-KEY>
```

- If using global firewall rules, disable auto-firewall for the peer:

```
set vpn ipsec site-to-site peer <PeerID> auto-firewall no
```

- IKE group for the peer:

```
set vpn ipsec site-to-site peer <PeerID> ike-group <IKE-GRP-NAME>
```

- IP address of the ACM WAN interface:

```
set vpn ipsec site-to-site peer <PeerID> local-ip <WAN-IP-ADDRESS>
```

- Define at least one tunnel for this peer:

```
set vpn ipsec site-to-site peer <PeerID> tunnel 1
```

- ESP group for the peer's tunnel(s) (this must be set for each of the peer's tunnels — see previous point):

```
set vpn ipsec site-to-site peer <PeerID> tunnel 1 esp-group <ESP-GRP-NAME>
```

- The private subnet behind ACM. In general, this is the enterprise LAN:

```
set vpn ipsec site-to-site peer <PeerID> tunnel 1 local subnet <LAN-SUBNET/SUBNET-BITMASK>
```

- Use the AirLink router's LAN-subnet as the remote subnet:

```
set vpn ipsec site-to-site peer <PeerID> tunnel 1 remote subnet <oMG-LAN-SUBNET/SUBNET-BITMASK>
```

VPN ID

When ACM is located within a DMZ, behind an external firewall, the VPN connection is set up to an external IP address that is translated to an internal private address (the *outside* interface of ACM). To specifically identify the peer of the connection, the peer must be configured with a *Server ID* and this ID must match that of ACM.

The default behavior in ACM is to use the local IP of the outside interface address as this ID.

However the ID can be explicitly assigned another value. This is a good practice as it allows the ACM internal IP address to be re-assigned without requiring the peers to also be reconfigured in the event that the enterprise network is re-arranged after deployment.

Configure the ACM ID:

```
set vpn ipsec site-to-site peer any authentication id <IDENTITY-STRING>
```

Certificate Management and Revocation

ACM can utilize a system of public key and certificates to allow or deny access to client devices. For a client device to connect to ACM, its certificate must be signed by the same CA authority and must have the same cacert.pem certificate file that ACM has. These certificates and their associated keys are issued by a certificate authority (CA).

ACM supports the following certificate types:

- RSA 2048 bits

- RSA 3072 bits
- ECDSA 224 bits (Note: Not supported by oMG/MG90)

To provision ACM with certificates:

1. Copy the certificates into the directory: /config/auth on ACM. To do so, log in to the server where the certificate files exist and invoke the following commands:
```
[user@server ~]$ scp -P 2222 <ca_cert_file_name> admin@<ACM-IP>:/config/auth
[user@server ~]$ scp -P 2222 <ACM_cert_file_name> admin@<ACM-IP>:/config/auth
[user@server ~]$ scp -P 2222 <ACM_key_file_name> admin@<ACM-IP>:/config/auth
```
2. Provision the CA certificates:
```
set vpn ipsec x509 ca <ca_cert_name> ca-cert-file /config/auth/<ca_cert_file_name>
set vpn ipsec x509 ca <ca_cert_name> ca-cert-type <RSA | ECDSA>
```
3. Provision the host certificate:
```
set vpn ipsec x509 host <host_cert_name> cert-file /config/auth/<ACM_cert_file_name>
set vpn ipsec x509 host <host_cert_name> cert-type <RSA | ECDSA>
set vpn ipsec x509 host <host_cert_name> key file /config/auth/<ACM_key_file_name>
set vpn ipsec x509 host <host_cert_name> key type <RSA | ECDSA>
```

As part of this security system, ACM also supports a certificate revocation list (CRL) that explicitly lists the certificates of devices who should not be granted access to ACM. The certificates listed can be either revoked (denied access) or in a "hold" state meaning they have yet to be approved and are thus temporarily invalid.

To use the CRL on ACM:

1. Copy the CRL file into the directory: /config/auth on ACM. To do so, log in to the server where the CRL file exists and invoke the following command:
```
[user@server ~]$ scp -P 2222 <crl_file> admin@<ACM-IP>:/config/auth
```
2. Configure the CRL on ACM:
```
set vpn ipsec x509 ca <ca_cert_name> crl-file /config/auth/<crl_file>
```

ACM Server High Availability

ACM supports two 'high availability' methods (VRRP and DNS Load Balancing), which can ensure ACM services remain available in case of server failures (both methods) or heavy loads (DNS load balancing). For details, including supported devices, refer to the *AirLink Connection Manager High Availability Setup Guide (Document #4118775)*, (available from the ACM device page on the Source (source.sierrawireless.com/devices/airlink-vpn/acm-vpn-server).

Client-side (VPN Peers) VPN Configuration

VPN peers must be configured to work with ACM as described in the following sections:

- AirLink oMG/MG90 Router Support
- AirLink Router Support — ES, GX, LX, MP, RV Series
- AirLink Router Support — RX55, XR Series
- NCP Secure Entry Client for Windows

AirLink oMG/MG90 Router Support

This section applies to AirLink oMG2000/500 and MG90.

oMG/MG90 IKE/ESP Negotiation Parameters

When using oMG/MG90 peers with ACM, some limitations apply:

- Some ACM features are not supported by oMG/MG90.
- Some oMG/MG90 features are not supported by ACM.

The following table describes these limitations and the restrictions these place on ACM configuration and oMG/MG90 configuration.

Table 5-3: oMG/MG90 IKE/ESP Parameter Support

	ACM 3.1.1 non-FIPS		ACM 3.1.1 FIPS		oMG non-FIPS		oMG FIPS		MG90 non-FIPS		MG90 FIPS		
Type	IKE	ESP	IKE	ESP	IKE	ESP	IKE	ESP	IKE	ESP	IKE	ESP	Setup Requirements
Encryption													
aes128	Y	Y	Y	Y	Y	Y	Y	—	Y	Y	Y	Y	
aes128ccm16	—	—	—	Y[a]	—	—	—	—	—	—	—	—	
aes128gcm16	Y[a]	Y[a]	Y[a]	Y[a]	—	—	—	Y	Y[b]	Y[b]	—	Y[a]	
aes192	Y	Y	Y	Y	—	—	—	—	—	—	—	—	
aes192gcm16	Y	Y	Y	Y	—	—	—	—	—	—	—	—	
aes256	Y	Y	Y	Y	Y	Y	—	—	Y	Y	Y	Y	
aes256ccm16	—	—	—	Y[a]	—	—	—	—	—	—	—	—	
aes256gcm16	Y[a]	Y[a]	Y[a]	Y[a]	—	—	—	—	Y[b]	Y[b]	—	Y[a]	
3des	Y[c]	Y[c]	—	—	Y	Y	—	—	Y	Y	—	—	
Hash													
sha1	Y[c]	Y[c]	—	—	Y	Y	—	—	Y	Y	—	—	
sha2_256	Y	Y	Y	Y	Y	Y	Y	—	Y	Y	Y	Y	
sha2_384	Y	Y	Y	Y	—	—	—	—	—	—	—	—	
sha2_512	Y	Y	Y	Y	Y	Y	—	—	Y	Y	Y	Y	
md5	Y[c]	Y[c]	—	—	Y	Y	—	—	Y	Y	—	—	
none	—	—	—	Y[a]	—	—	—	Y	—	—	—	Y[a]	

Table 5-3: oMG / MG90 IKE / ESP Parameter Support (Continued)

Type	ACM 3.1.1 non-FIPS		ACM 3.1.1 FIPS		oMG non-FIPS		oMG FIPS		MG90 non-FIPS		MG90 FIPS		Setup Requirements
	IKE	ESP	IKE	ESP	IKE	ESP	IKE	ESP	IKE	ESP	IKE	ESP	
DH Group													
1	—	—	—	—	—	—	—	—	—	—	—	—	On ACM, make sure the dh-group is configured in esp-group proposals.
2	Y[c]	Y[c]	—	—	Y	—	—	—	Y	Y[d]	—	—	
5	Y[c]	Y[c]	—	—	Y	—	—	—	Y	Y[d]	—	—	
14	Y	Y	Y	Y	Y	—	—	—	Y	Y[d]	Y	Y	
15	Y	Y	Y	Y	Y	—	—	—	Y	Y[d]	Y	Y	
16	Y	Y	Y	Y	Y	—	—	—	Y	Y[d]	Y	Y	
17	Y	Y	Y	Y	Y	—	—	—	Y	Y[d]	—	—	
18	Y	Y	Y	Y	—	—	—	—	Y	Y[d]	—	—	
19	Y	Y	Y	Y	—	—	Y	—	Y[b]	Y[b]	Y	Y	
20	Y	Y	Y	Y	—	—	—	—	—	—	Y	Y	
21	Y	Y	Y	Y	—	—	—	—	—	—	Y	Y	
26	Y	Y	Y	Y	—	—	—	—	—	—	—	—	
none	—	Y[e]	—	—	—	Y	—	Y	—	Y[e]	—	—	

a. When aes128ccm16, aes128gcm16, aes256ccm16, or aes256gcm16 encryption is used, hash must be none.
b. Supported on MG90 LTE, MG90 LTE-A Pro, MG90-5G
c. Indicated cryptographic protocols are less secure than other options and are not recommended.
d. ESP DH group support is available in MGOS 4.1.x and higher. In versions before 4.1, the DH group for ESP is inherited from IKE, and after a re-key, no DH group is applied to the ESP.
e. DH group 'none' is not recommended. For greater security, choose a supported ESP DH group.

AirLink Router Support — ES, GX, LX, MP, RV Series

This section applies to AirLink ES, GX, LX, MP, and RV series routers.

ACM / AirLink (ES, GX, LX, MP, RV Series) Setup Requirements

When using AirLink ES, GX, LX, MP or RV series routers with ACM, some limitations apply:

- Some ACM features are not supported by the AirLink devices.
- Some AirLink features are not supported by ACM.

The following tables describe these limitations and the restrictions these place on ACM configuration and AirLink configuration (using ACEmanager).

Table 5-4: AirLink (ES, GX, LX[a], MP, RV) IKE / ESP Parameter Support

Type	ACM 3.1.1 (non-FIPS)		ACM 3.1.1 (FIPS)[a]		AirLink		Setup Requirements
	IKE	ESP	IKE	ESP	IKE	ESP	
Encryption							
aes128	Y	Y	Y	Y	Y	Y	
aes128ccm16	—	—	—	Y[b]	—	—	
aes128gcm16	Y[b]	Y[b]	Y[b]	Y[b]	—	—	
aes192	Y	Y	Y	Y	Y	Y	
aes192gcm16	Y	Y	Y	Y	—	—	
aes256	Y	Y	Y	Y	Y	Y	
aes256ccm16	—	—	—	Y[b]	—	—	
aes256gcm16	Y[b]	Y[b]	Y[b]	Y[b]	Y	Y	
3des	Y[c]	Y[c]	—	—	Y	Y	
des	—	—	—	—	—	—	
none	—	—	—	—	Y	Y	
Hash							
sha1	Y[c]	Y[c]	—	—	Y	Y	
sha2_256	Y	Y	Y	Y	Y	Y	
sha2_384	Y	Y	Y	Y	Y	Y	
sha2_512	Y	Y	Y	Y	Y	Y	
md5	Y[c]	Y[c]	—	—	Y	Y	
none	—	—	—	Y[b]	Y	Y	

Table 5-4: AirLink (ES, GX, LX[a], MP, RV) IKE / ESP Parameter Support (Continued)

Type	ACM 3.1.1 (non-FIPS)		ACM 3.1.1 (FIPS)[a]		AirLink		Setup Requirements
	IKE	ESP	IKE	ESP	IKE	ESP	
DH Group							
1	—	—	—	—	Y	Y	On ACM, make sure the dh-group is configured in esp-group proposals.
2	Y[c]	Y[c]	—	—	Y	Y	
5	Y[c]	Y[c]	—	—	Y	Y	
14	Y	Y	Y	Y	Y	Y	
15	Y	Y	Y	Y	Y	Y	
16	Y	Y	Y	Y	Y	Y	
17	Y	Y	Y	Y	Y	Y	
18	Y	Y	Y	Y	Y	Y	
19	Y	Y	Y	Y	Y	Y	
20	Y	Y	Y	Y	Y	Y	
21	Y	Y	Y	Y	Y	Y	
26	Y	Y	Y	Y	Y	Y	
none	—	Y[d]	—	—	Y	Y	

a. FIPS is not supported by LX40 or LX60 routers.
b. When aes128ccm16, aes128gcm16, aes256ccm16, or aes256gcm encryption is used, hash must be none.
c. Indicated cryptographic protocols are less secure than other options and are not recommended.
d. DH group 'none' is not recommended. For greater security, choose a supported ESP DH group.

Table 5-5: Additional ACM / AirLink Setup Requirements

Feature	Support limitation	Setup Requirement
Certificates	AirLink devices do not support certificates	On ACM, configure the peer to use PSK only.
DNS Load Balancing	AirLink devices do not support load balancing	n/a

'Single Address' Type for Host2LAN Connection

Typically, AirLink routers are configured to use LAN2LAN VPN connections, which allows the AirLink device and its client devices to access the VPN tunnel.

However, if the AirLink device must be configured to use a Host2LAN VPN connection (where only the AirLink device can access the tunnel), the device must be configured to use the "Single Address" local address type, and the address must match the device's USB IP address or Ethernet IP address to establish a tunnel to ACM.

1. Check and update (if necessary) the IP address that will be used:
   - USB IP address:
     i. In ACEmanager, select LAN > USB.
     ii. In USB Device Mode, make sure USBNET is selected.

iii. In Device USB IP, enter the AirLink device's IP address.
The default address is 192.168.14.31. If the router is part of a fleet, each router must be configured with a unique address — modify the third and/or fourth octets for each device (modify one octet for up to 256 routers, or both octets for 255+ routers).

iv. Click Apply.

- Ethernet IP address:

i. In ACEmanager, select LAN > Ethernet.

ii. In Device IP, enter the AirLink device's IP address.
The default address is 192.168.13.31. If the router is part of a fleet, each router must be configured with a unique address — modify the third and/or fourth octets for each device (modify one octet for up to 256 routers, or both octets for 255+ routers).

iii. Click Apply.

2. Select VPN > [VPN#].
   a. In VPN 1 type, select IPsec Tunnel.
   b. In Local Address Type, select "Single Address" from the drop-down list.
   c. In Local Address, enter the IP address (USB or Ethernet) set in step 1.
   d. Click Apply.
   e. Click Reboot.

Main/Aggressive Mode Configuration

AirLink routers support IKEv1 in main mode and aggressive mode.

When determining whether to configure an AirLink device for aggressive mode, consider the following use cases:

Table 5-6: Main/Aggressive Mode Use Cases

Main Mode	Main Mode + FQDN	Aggressive Mode
▪ Secure ▪ Available only if ID Authentication ID Type is Static IP address	▪ Secure ▪ Best option if Static IP address is not available. ▪ All routers use the same PSK — If PSK is compromised, all routers in fleet must be configured with a new PSK.	▪ Not secure, PSK transmitted unencrypted in Phase 1. ▪ Routers can use different PSKs ▪ If user accepts the security risk, this option allows for faster setup. *Note: Not supported for certificate authentication.*

For each device configured to use aggressive mode, configure ACM using:

```
set vpn ipsec site-to-site peer <PeerID> authentication aggressivemode yes
```

(See Table 5-2 on page 42 for supported <PeerID> types and formats.)

AirLink Router Support — RX55, XR Series

This section applies to AirLink RX55 and XR series routers.

ACM / AirLink (RX55, XR Series) Setup Requirements

When using AirLink RX55 or XR Series routers with ACM, some limitations apply:

- Some ACM features are not supported by RX55 or XR routers.
- Some AirLink features are not supported by ACM.

The following tables describe these limitations and the restrictions these place on ACM configuration and AirLink configuration (using AirLink OS).

Table 5-7: AirLink XR Series IKE / ESP Parameter Support

Type	ACM 3.1.1 (non-FIPS)		ACM 3.1.1 (FIPS)		RX55 / XR Series		Setup Requirements
	IKE	ESP	IKE	ESP	IKE	ESP	
Encryption							
aes128	Y	Y	Y	Y	Y	Y	
aes128ccm16	—	—	—	Y[a]	—	—	
aes128gcm16	Y[a]	Y[a]	Y[a]	Y[a]	Y	Y	
aes192	Y	Y	Y	Y	Y	Y	
aes192gcm16	Y	Y	Y	Y	Y	Y	
aes256	Y	Y	Y	Y	Y	Y	
aes256ccm16	—	—	—	Y[a]	—	—	
aes256gcm16	Y	Y	Y[a]	Y[a]	Y	Y	
3des	Y[b]	Y[b]	—	—	—	—	
des	—	—	—	—	—	—	
none	—	—	—	—	—	—	
Hash							
sha1	Y[b]	Y[b]	—	—	—	—	
sha2_256	Y	Y	Y	Y	Y	Y	
sha2_384	Y	Y	Y	Y	Y	Y	
sha2_512	Y	Y	Y	Y	Y	Y	
md5	Y[b]	Y[b]	—	—	—	—	
none	—	—	—	Y[a]	—	—	

Table 5-7: AirLink XR Series IKE / ESP Parameter Support (Continued)

Type	ACM 3.1.1 (non-FIPS)		ACM 3.1.1 (FIPS)		RX55 / XR Series		Setup Requirements
	IKE	ESP	IKE	ESP	IKE	ESP	
DH Group							
1	—	—	—	—	—	—	On ACM make sure the dh-group is configured in esp-group proposals
2	Y[b]	Y[b]	—	—	—	—	
5	Y[b]	Y[b]	—	—	—	—	
14	Y	Y	Y	Y	Y	Y	
15	Y	Y	Y	Y	Y	Y	
16	Y	Y	Y	Y	Y	Y	
17	Y	Y	Y	Y	Y	Y	
18	Y	Y	Y	Y	Y	Y	
19	Y	Y	Y	Y	Y	Y	
20	Y	Y	Y	Y	Y	Y	
21	Y	Y	Y	Y	Y	Y	
26	Y	Y	Y	Y	Y	Y	
none	—	Y[c]	—	—	—	—	

a. When aes128ccm16, aes128gcm16, aes256ccm16, or aes256gcm encryption is used, hash must be none.
b. Indicated cryptographic protocols are less secure than other options and are not recommended.
c. DH group 'none' is not recommended. For greater security, choose a supported ESP DH group.

NCP Secure Entry Client for Windows

ACM supports VPN connections from mobile devices using NCP Secure Entry Client for Windows.

For NCP client configuration details, refer to the *AirLink Connection Manager Configuration Guide for NCP Secure Entry Client (Document #4118774)*, available from the ACM device page on source.sierrawireless.com/devices/airlink-vpn/acm-vpn-server/.

For NCP Client product support, refer to https://www.ncp-e.com.

NCP Client / ACM Setup Requirements

When using NCP Client peers with ACM, some limitations apply:

- Some ACM features are not supported by NCP.
- Some NCP features are not supported by ACM.

The following table describes these limitations and the restrictions these place on ACM configuration and NCP configuration.

Table 5-8: NCP Client IKE / ESP Parameter Support

Type	ACM 3.1.1 non-FIPS		ACM 3.1.1 FIPS		NCP Client non-FIPS		NCP Client FIPS		Setup Requirements
	IKE	ESP	IKE	ESP	IKE	ESP	IKE	ESP	
Encryption									
aes128	Y	Y	Y	Y	Y	Y	Y	Y	
aes128ccm16	—	—	—	Y[a]	—	—	—	—	
aes128gcm16	Y[a]	Y[a]	Y[a]	Y[a]	—	—	—	Y	
aes192	Y	Y	Y	Y	—	—	—	—	
aes192gcm16	Y	Y	Y	Y	—	—	—	—	
aes256	Y	Y	Y	Y	Y	Y	Y	Y	
aes256ccm16	—	—	—	Y[a]	—	—	—	—	
aes256gcm16	Y[a]	Y[a]	Y[a]	Y[a]	—	—	—	Y	
3des	Y[b]	Y[b]	—	—	Y	Y	—	—	
des	—	—	—	—	Y	Y	—	—	
Hash									
sha1	Y[b]	Y[b]	—	—	Y	Y	—	—	
sha2_256	Y	Y	Y	Y	Y	Y	Y	Y	
sha2_384	Y	Y	Y	Y	—	—	—	—	
sha2_512	Y	Y	Y	Y	Y	Y	Y	Y	
md5	Y[b]	Y[b]	—	—	Y	Y	—	—	
none	—	—	—	Y[a]	—	Y	—	—	

Table 5-8: NCP Client IKE / ESP Parameter Support (Continued)

Type	ACM 3.1.1 non-FIPS		ACM 3.1.1 FIPS		NCP Client non-FIPS		NCP Client FIPS		Setup Requirements
	IKE	ESP	IKE	ESP	IKE	ESP	IKE	ESP	
DH Group									
1	—	—	—	—	Y	Y	—	—	On ACM, make sure the dh-group is configured in esp-group proposals.
2	Y[b]	Y[b]	—	—	Y	Y	—	—	
5	Y[b]	Y[b]	—	—	Y	Y	—	—	
14	Y	Y	Y	Y	Y	Y	Y	Y	
15	Y	Y	Y	Y	Y	Y	Y	Y	
16	Y	Y	Y	Y	Y	Y	Y	Y	
17	Y	Y	Y	Y	Y	Y	—	—	
18	Y	Y	Y	Y	Y	Y	—	—	
19	Y	Y	Y	Y	—	—	Y	Y	
20	Y	Y	Y	Y	—	—	Y	Y	
21	Y	Y	Y	Y	—	—	Y	Y	
26	Y	Y	Y	Y	—	—	—	—	
none	—	Y[c]	—	—	—	Y	Y	Y	

a. When aes128ccm16, aes128gcm16, aes256ccm16, or aes256gcm encryption is used, hash must be none.
b. Indicated cryptographic protocols are less secure than other options and are not recommended.
c. DH group 'none' is not recommended. For greater security, choose a supported ESP DH group.

Table 5-9: Additional ACM / NCP Client Setup Requirements

Feature	Support limitation	Setup Requirement
PFS	ACM always uses PFS	On the NCP Client, enable PFS.
Authentication	For certificate authentication, ACM supports only the NCP ID type "ASN1 Distinguished Name".	On the NCP Client, configure the ID type as "ASN1 Distinguished Name".
Certificates	NCP may not support RSA-3072.	On the NCP Client, configure to use RSA-2048. If RSA-3072 is attempted and fails, change to one of the other options.
	On NCP Client 10.1x, RFC7427 must be disabled to connect to an ACM using a certificate.	On the NCP Client, navigate to Profile Settings > Advanced IPsec Options and disable the option: Enable negotiating RFC7427 (digital signatures)
Peer ID Type	ACM supports: ▪ Fully Qualified Domain Name ▪ IP Address ▪ Fully Qualified Username ▪ ASN1 Distinguished Name	On the NCP Client, use one of: ▪ FQDN (recommended) ▪ ASN1 Distinguished Name (required for certificate authentication) ▪ IP Address ▪ Fully Qualified Username

Configuring ACM for NCP Secure Entry Client for Windows

To use the NCP Secure Entry Client for Windows with ACM, you must ensure ACM and the client are configured appropriately. For server-side and client-side configuration instructions, refer to the *AirLink Connection Manager Configuration Guide for NCP Secure Entry Client (Document #4118774)*, available on source.sierrawireless.com/devices/airlink-vpn/acm-vpn-server/.

6: Troubleshooting

Upgrading to ACM 3.1.1 (non-FIPS) or ACM 3.1.1 (FIPS)

When upgrading to ACM 3.1.1 (non-FIPS) or ACM 3.1.1 (FIPS), you must enter a name to store the image file.

To upgrade to ACM 3.1.1 (non-FIPS) or ACM 3.1.1 (FIPS) from an earlier version:

1. Enter the following command:
   `add system image <imagefile>`

   (where <imagefile> is the pathname of an ISO file (such as " acm-3.1.1.0-20240709.1-amd64.iso" or "acm-3.1.1.0-20240709.FIPS.1-amd64.iso") on ACM or a URL to a remote file)
2. When prompted to enter a name for the image, use the version portion of the <imagefile> name (e.g. "3.1.1.0-20240709.1" or "3.1.1.0-20240709.FIPS.1"), or an alternate name of your choice, and press Enter to continue.

> *Note: The name must contain only letters, digits, and special characters ('-', '+', '.', '_').*

Examples (**bolded** text represents your input):

- Upgrading to ACM 3.1.1 (non-FIPS):

```
admin@ACM:~$ add system image ACM-3.1.1.0-20240709.1-amd64.iso
Checking MD5 checksums of files on the ISO image...OK.
...
What would you like to name this image? []: 3.1.1.0-20240709.1
...
```

- Upgrading to ACM 3.1.1 (FIPS):

```
admin@ACM:~$ add system image ACM-3.1.1.0-20240709.FIPS.1-amd64.iso
Checking MD5 checksums of files on the ISO image...OK.
...
What would you like to name this image? []: 3.1.1.0-20240709.FIPS.1
...
```

View VPN Configuration Details

Use the following commands to view various aspects of the VPN configuration.

IKE Process Status

To view the status of the IKE process:

```
admin@ACM: show vpn ike status

Charon Process Running
Charon PID: 14981
```

IKE Security Associations

To view IKE security associations:

```
admin@ACM: show vpn ike sa
Peer ID / IP            Local ID / IP
------------            -------------
CN=omg_valid1           192.168.4.22

    State  Encrypt  Hash  D-H Grp  NAT-T  A-Time  L-Time
    -----  -------  ----  -------  -----  ------  ------
    up     aes256   sha1  5        no     n/a     0

Peer ID / IP            Local ID / IP
------------            -------------
192.100.1.2             192.168.4.22

    State  Encrypt  Hash  D-H Grp  NAT-T  A-Time  L-Time
    -----  -------  ----  -------  -----  ------  ------
    up     aes256   sha1  5        yes    15942   28800
```

IPsec Process Status

To view the status of the IPsec process:

```
admin@ACM: show vpn ipsec status

Charon Process Running PID: 14981
1 Active IPsec Tunnels

IPsec Interfaces :
       eth0    (192.168.4.10)
       eth1    (no IP on interface statically configured as local-ip for any VPN peer)
```

IPsec Security Associations

To view IPsec security associations:

```
admin@ACM: show vpn ipsec sa

Peer ID / IP           Local ID / IP
------------           -------------


Peer ID / IP           Local ID / IP
------------           -------------
CN=omg_revoked1        192.168.4.22

    Tunnel State Bytes Out/In Encrypt Hash NAT-T A-Time L-Time Proto
    ------ ----- ------------ ------- ---- ----- ------ ------ -----
    7      down  n/a          n/a     n/a  no    n/a    0       all


Peer ID / IP           Local ID / IP
------------           -------------
CN=omg_valid1          192.168.4.22

    Tunnel State Bytes Out/In Encrypt Hash NAT-T A-Time L-Time Proto
    ------ ----- ------------ ------- ---- ----- ------ ------ -----
    1      up    71.4K/71.8K  aes128  sha1 no    n/a    0      all


Peer ID / IP           Local ID / IP
------------           -------------
192.100.1.2            192.168.4.22
    Tunnel State Bytes Out/In Encrypt Hash NAT-T A-Time L-Time Proto
    ------ ----- ------------ ------- ---- ----- ------ ------ -----
    2      up    233.6K/232.0K aes128  sha1 yes   2152   3600   all
```

IPsec IP Pool Status

To view IPsec security associations:

```
admin@ACM: show vpn ipsec ip-pool

Leases in pool '192.168.114.0/24', usage: 3/254, 0 online
192.168.114.2 offline 'TestNCP2'
192.168.114.1 offline 'peapuser'
192.168.114.3 offline 'C=CA, ST=BC, O=InMotion, OU=eng, CN=Ttest1'
Leases in pool '10.101.1.0/24', usage: 0/254, 0 online
no matching leases found
```

Debug Information

To view more detailed information when you are troubleshooting, use the *show vpn debug* command (for all debug information) or the *show vpn debug peer <PeerID>* command (to debug a specific peer):

```
admin@ACM: show vpn debug

Status of IKE charon daemon (strongSwan 5.5.3, Linux 4.19.181-amd64-vyos, x86_64):
 uptime: 3 hours, since Sep 07 09:37:38 2022
 malloc: sbrk 2973696, mmap 0, used 934864, free 2038832
 worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0, scheduled: 0
 loaded plugins: charon test-vectors ldap pkcs11 aesni aes rc2 sha2 sha1 md5 rdrand
       random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp
       dnskey sshkey pem openssl gcrypt af-alg fips-prf gmp curve25519 agent xcbc
       cmac hmac ctr c cm gcm curl attr kernel-netlink resolve socket-default
       connmark farp stroke vici updown eap-identity eap-aka eap-md5 eap-gtc e ap-
       mschapv2 eap-radius eap-tls eap-ttls eap-tnc xauth-generic xauth-eap xauth-pam
       xauth-noauth tnc-tnccs dhcp lookip error-not ify certexpire led addrblock
       unity
Virtual IP pools (size/online/offline):
  172.18.114.0/24: 254/1/1
Listening IP addresses:
  10.1.65.114
  192.168.114.1
  10.1.97.114
Connections:
peer-any-tunnel-1:  10.1.65.114...%any  IKEv2
peer-any-tunnel-1:   local:  [10.1.65.114] uses pre-shared key authentication
peer-any-tunnel-1:   remote: uses EAP_RADIUS authentication with EAP identity '%any'
peer-any-tunnel-1:   child:  192.168.114.0/24 === dynamic TUNNEL
Security Associations (1 up, 0 connecting):
peer-any-tunnel-1[19]: ESTABLISHED 72 seconds ago,
       10.1.65.114[10.1.65.114]...10.1.65.66[]
peer-any-tunnel-1[19]: IKEv2 SPIs: 89f07750b7bb0459_i 6cd14c493a517903_r*, rekeying
       disabled
peer-any-tunnel-1[19]: IKE proposal: AES_CBC_256/HMAC_SHA1_96/PRF_HMAC_SHA1/
       MODP_1536
peer-any-tunnel-1{30}:  INSTALLED, TUNNEL, reqid 5, ESP in UDP SPIs: c85fcdca_i
       25b11ae1_o
peer-any-tunnel-1{30}:  AES_CBC_256/HMAC_SHA1_96, 384 bytes_i (8 pkts, 2s ago), 384
```

Dead Peer Detection is not Working

If dead peer detection (DPD) is not functioning properly:

- Make sure the correct “set vpn ipsec” DPD options are used:
  - When enabling DPD, use “action clear” — do not use “action hold” or “action reset”.
    For example:
    ```
    set vpn ipsec ike-group <IKE-GRP-NAME> dead-peer-detection action clear
    ```
  - If using IKEv1, use “dead-peer-detection interval” and “dead-peer-detection timeout”. See Configure IKE Groups with IKEv1 on page 39.

- If using IKEv2, use “ikev2-retransmit-timeout” and “ikev2-retransmit-tries”. See Configure IKE Groups with MOBIKE (IKEv2) on page 38.

vpn ipsec ‘lifetime’ Command is Not Available

The ‘lifetime command is no longer supported for either IKEv1 or IKEv2 and has been removed.

VPN Tunnel Establishes with Mismatched IKE Group

Note: This issue applies to IKEv1 and IKEv2.

If ACM is configured with multiple IKE groups (e.g group_1, group_2) and has configured a peer with one of those groups (e.g. group_1), a VPN tunnel will be established if the peer uses any of the configured IKE groups.

For example:

- On ACM:
  - ACM configured with IKE groups group_1 and group_2
  - ACM configures peer with group_1
- On the peer:
  - If peer is configured to use group_1, a tunnel will establish (peer’s configuration matches ACM’s configuration for the peer).
  - If the peer is configured to use group_2, a tunnel will establish (peer’s configuration does not match ACM’s configuration for the peer, but does match one of the groups configured on ACM).
  - If the peer is configured to use group_3, a tunnel will fail to establish because ACM is not configured with group_3.

NCP Certificate Authentication Failed — "No trusted RSA public key"

For NCP certification authentication to work with ACM, NCP must be configured to use ID Type "ASN1 Distinguished Name". For details, refer to the *AirLink Connection Manager Configuration Guide for NCP Secure Entry Client (Document #4118774)*, available on source.sierrawireless.com/devices/airlink-vpn/acm-vpn-server/.

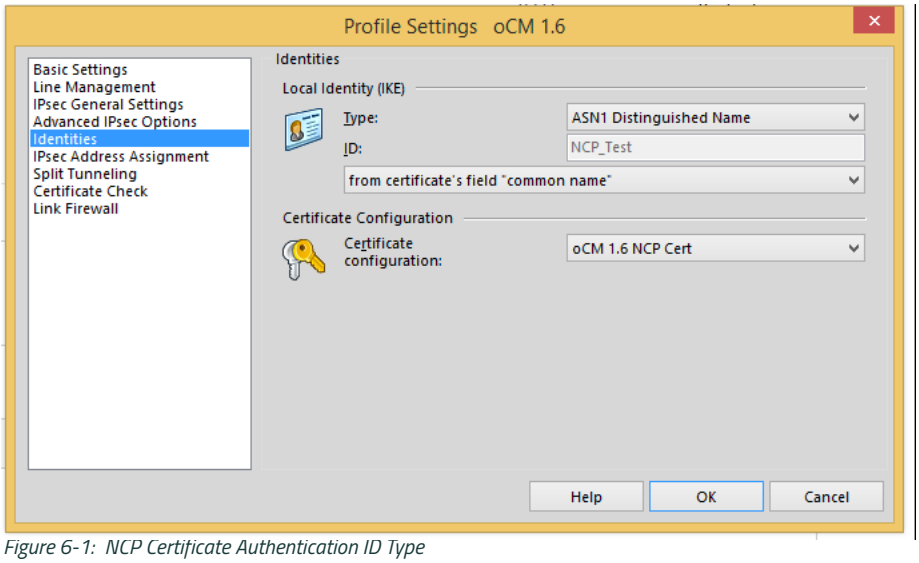


Figure 6-1: NCP Certificate Authentication ID Type

A: Important ACM Configuration Requirements

As noted in Connecting to ACM from an Inside Device on page 24, the information described below is required for the initial configuration of ACM so that it can be installed inside a customer network, boot successfully, and be accessible for further configuration.

The following items must be configured before ACM can accept connections.

Table A-1: Required ACM Configuration Items

Item	Note	Example
Outside IP address and netmask	This address must be accessible from the mobile network. In most cases, this is a globally routable IP address.	
Outside default gateway	Needed in most cases. To be discussed prior to shipping if this is not desired.	
Public DNS server	Defaulted to opendns.org server	
Public NTP server	Defaulted to public NTP pool	server 0.us.pool.ntp.org
Inside IP address and netmask	This must be compatible with your enterprise LAN address.	The default settings are 10.99.0.1/24.
Next hop address	Required if you have an intermediate router between ACM and your application servers that are on a different network than that of the ACM inside address.	10.99.0.2

The enterprise network will have existing default routing rules that specify how traffic from LAN devices is routed, usually toward the Internet. When an ACM is introduced, the mobile address space will only be accessible via ACM. ACM's *Next Hop Address* specifies how mobile traffic will reach the enterprise. For enterprise traffic to reach the mobile network via the VPN, a reverse route must be added at the intermediate router (between ACM and an enterprise application).

ACM is shipped with a default configuration template including an example VPN connection specification. The example may be modified or a new VPN connection can be defined. However, for the VPN connection to provide a communication channel that will pass data beyond itself, the mobile address space and the enterprise address space must be specified for your particular situation.

Table A-2: Address Space (Mobile and Enterprise) Definitions

Item	Note	Example
Mobile subnetwork(s)	Each AirLink router has an entire subnetwork. For small implementations, a class C address can be assigned to each device.	172.22.0.0/24 ... 172.22.255.0/24
Enterprise subnetwork(s)	If all mobile traffic must be routed through the VPN (full tunnel) it needs to be specified as 0.0.0.0/0 If some mobile traffic should be allowed to bypass the tunnel, then the tunneled traffic must be specified.	10.10.0.0/16

B: Hardware and VM Server Requirements

For ACM VPN appliances (VM or physical server) to provide reasonable performance, the minimum hardware specifications detailed below must be met.

VM Server Specifications

A server device hosting ACM as a virtual machine on VMWare vSphere (ESXi) 6.5+ must meet the following minimum specifications (to support up to 1000 concurrent active tunnels with a tunnel creation rate of 100 tunnels/min):

- vCPU cores: 8 dedicated cores
- vRAM size: 16 GB
- Available hard disk space: 16 GB

Note: To support larger numbers of concurrent tunnels, additional vCPU cores, vRAM, and hard disk space will be required.

Physical Server Specifications

A physical ACM server must meet the following minimum specifications:

- CPU — 3.3 GHz, 8 cores
- Memory — 16 GB RAM
- Storage:
  - HDD (7200 rpm) or SSD; ACM application requires 16 GB (minimum)
  - RAID 1 or RAID 5 is strongly recommended
- Ethernet — 2x 1 Gbps Ethernet ports
- Power — Dual power supplies are strongly recommended for redundancy
- Support for Linux software image