# AirLink Connection Manager (ACM)

## Installation and Operations Guide

SIERRA WIRELESS®

41111747
Rev 1

## Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the Sierra Wireless modem are used in a normal manner with a well-constructed network, the Sierra Wireless modem 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 modem, or for failure of the Sierra Wireless modem to transmit or receive such data.

## 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 InterDigital Group and MMP Portfolio Licensing.

## Copyright



## 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/<br>Global toll-free number: 1-877-687-7795<br>6:00 am to 6:00 pm PST |
| Corporate and product information | Web: sierrawireless.com |

## Revision History

| Revision number | Release date | Changes |
|---|---|---|
| 1 | December 2017 | • Document created |

# Contents

# 1: Introduction



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

## 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 physical server or as a virtual machine (VM) on VMWare vSphere (ESXi) 6.5+.

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

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

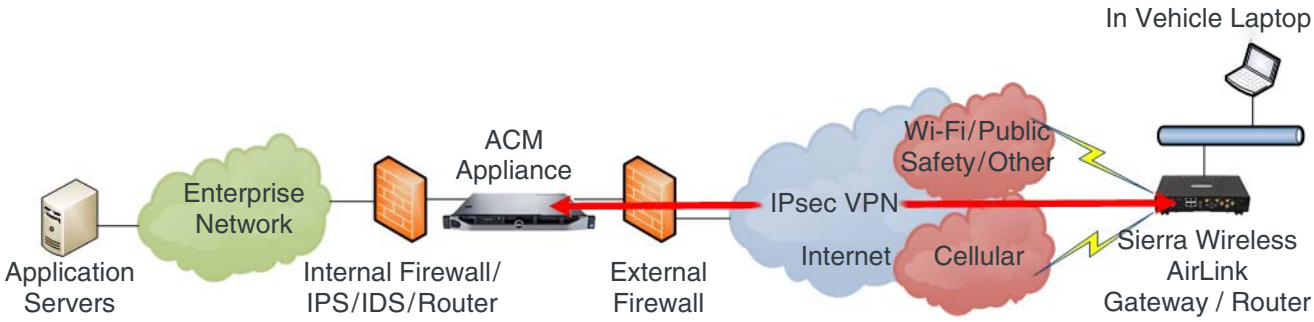



*Figure 1-1: The ACM fits between firewalls in an enterprise deployment*

The 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. When supported by the AirLink gateway/router, MOBIKE enables the device to establish a secure tunnel over any available wireless network, and as the vehicle moves and network access changes, the gateway/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: Not all AirLink devices support IKEv2. IKEv2 is supported on oMG2000/500 and MG90 routers.*

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

*Note: The ACM supports a subset of the commands and attributes described in the Vyatta VPN Reference Guide.*

## FIPS-Compliant ACM

ACM 2.0 is available in non-FIPS and FIPS-compliant configurations.

The FIPS-compliant ACM provides improved encryption capabilities and meets the requirements of the Federal Information Processing Standard 140-2, security level 1 (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2164.pdf).

# Supported VPN Peers (Endpoints)

VPN peers supported by the ACM include AirLink gateways/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).*

## Supported AirLink Gateways and Routers

This document applies to the device versions in the following table.

**Table 1-1: Supported Device Versions**

| AirLink Device | Software Versions Supported | |
|---|---|---|
| | ACM 2.0 (non-FIPS) | ACM 2.0 FIPS |
| oMG2000/500 Series | 3.12.1<br>3.14.3.2<br>3.14.4+ | 3.14.5+ |
| MG90 | 4.0.3+ | 4.1.0+ |
| MP70 | 4.6.1+ | Not supported |
| RV50 | 4.5.2+ | Not supported |
| GX440/GX450 | 4.4.4+<br>4.5.1+ | Not supported |
| GX400 | 4.4.1+ | Not supported |
| ES440/ES450 | 4.4.4+<br>4.5.1+ | Not supported |
| LS300 | 4.4.4+ | Not supported |

## Supported Mobile Client (NCP Client for Windows)

ACM 1.6 (and later) support 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.

# 2: Installation



This chapter describes how to install a physical ACM appliance or install an ACM VM on a VMWare vSphere server, and connect the ACM (physical or virtual) to your network.

## Physical ACM Appliance Requirements

The ACM dedicated appliance is a Dell PowerEdge R230XL (subject to future change).

### Environmental Requirements

The appliance must be installed in a temperature-controlled, computer data center environment. An external UPS power source is recommended. The unit's power supply is rated at 250W and a power cord is supplied.

### Mounting Requirements

The appliance is shipped with Dell-supplied rails that can be used to mount the unit in compatible 19" racks, or set onto securely mounted rack shelving.

### Ethernet Connection Requirements

Use Cat 5e Ethernet cabling with RJ45 connectors (not supplied) to connect the ACM Ethernet ports to the network infrastructure.

- Connect Port 1 (GB1), the outside interface, to the network connected to the enterprise firewall.
- Connect Port 2 (GB2), the inside interface, to the internal network.

*Note: Any additional ports that may be present are unused.*

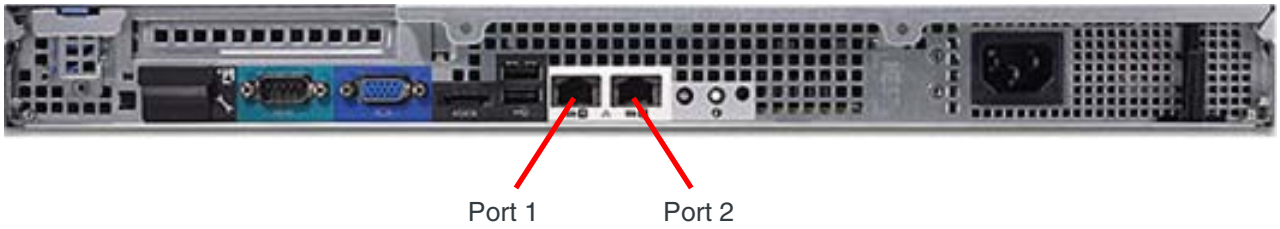



*Figure 2-1: Rear panel of ACM*

# ACM Virtual Machine Installation

The ACM virtual machine (VM) is available from Sierra Wireless for installation on a VMWare vSphere ESXi 6.5 server that has been configured as required for use with ACM.

## Virtual Machine Server Specifications

For the ACM to provide reasonable performance, the ESXi 6.5 server device must meet the following minimum specifications (to support up to 1000 concurrent tunnels):

- vCPU cores: 2
- vRAM size: 4 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 installing the ACM VM, you will need the following information from the ESXi 6.5 server:

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

## Installation Procedure

To install an ACM VM on the ESXi 6.5 server:

1. Contact your Sierra Wireless Support representative for instructions on downloading the ACM .ova file.
2. Using a Windows-based or Mac computer (Linux is not supported), open a browser and then connect to the vSphere Hypervisor client's address (for example, https://10.1.65.16). The vSphere Hypervisor client will appear.

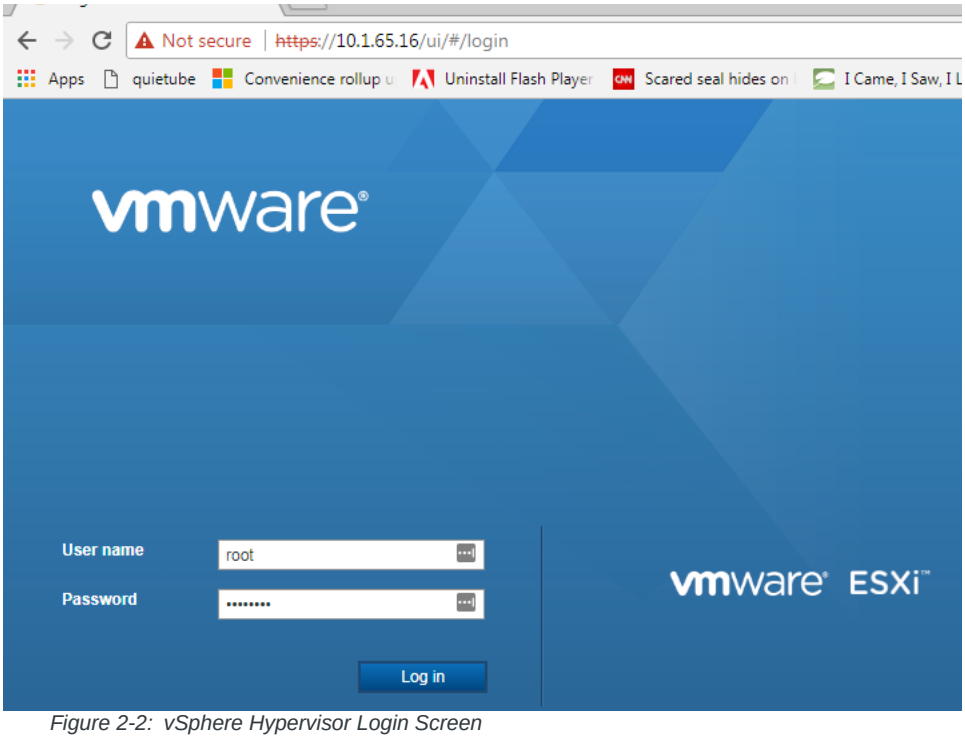



*Figure 2-2: vSphere Hypervisor Login Screen*

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

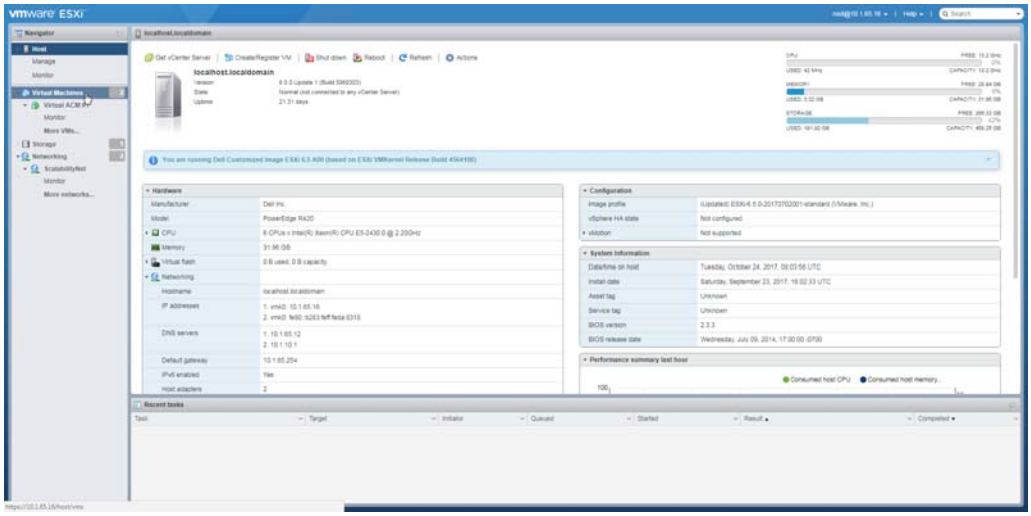
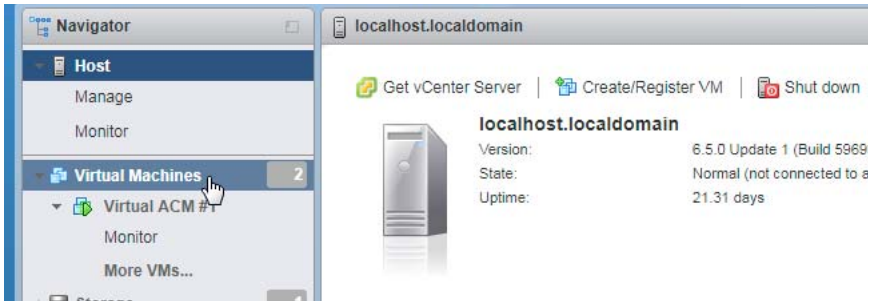
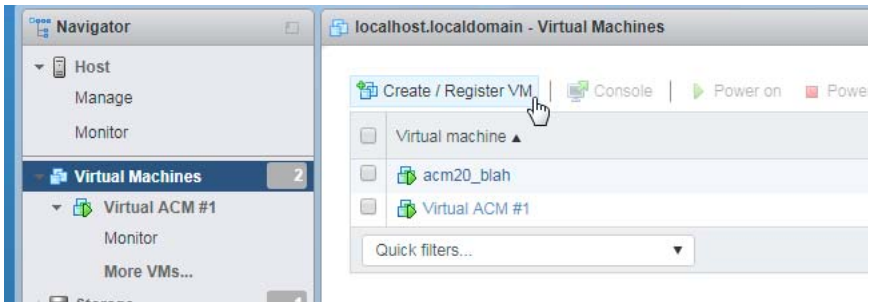



*Figure 2-3: vSphere Hypervisor Interface*

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

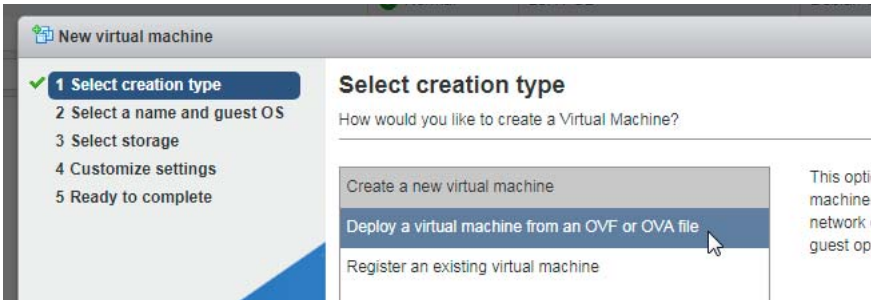



   b. In the Virtual Machines panel, click Create / Register VM.




   The New Virtual Machine wizard appears.

   c. In the Select creation type panel list, 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”.)

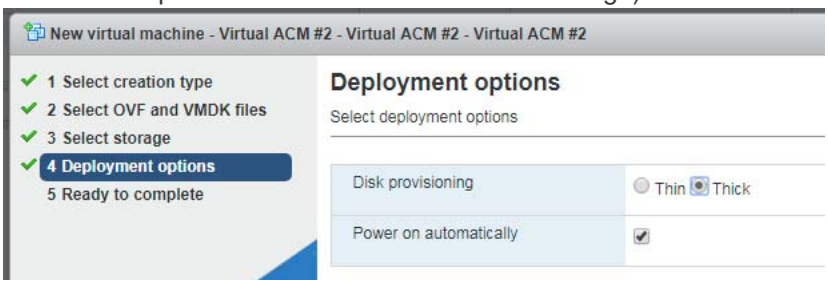
**f.** Click in the selection area to browse to (and select) the .ova file that you downloaded from Support, or drag and drop the .ova file into the selection area.

**g.** Click Next.

**h.** In the Select Storage screen, click Next.

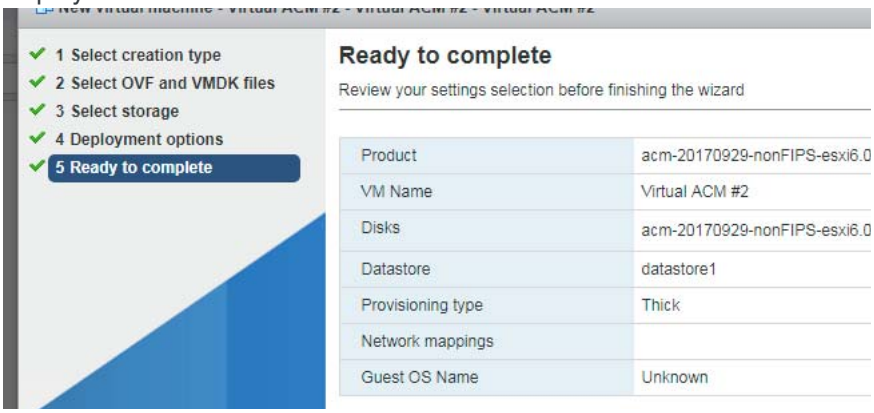
**i.** In the Deployment options panel, select:

- 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).

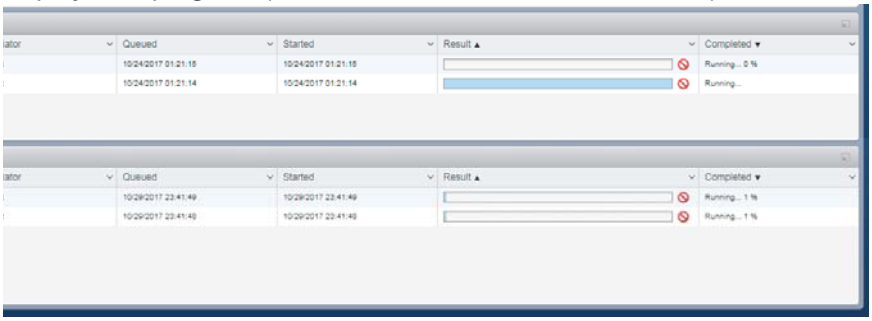



**j.** Click Next.

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

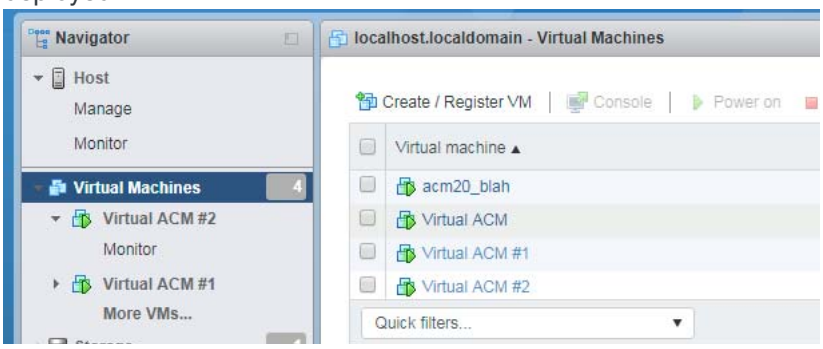



**l.** Wait for the ACM VM to deploy—Do NOT close the browser while the it is deploying. The status area at the bottom of the screen shows the deployment progress (this will take at least several minutes.)

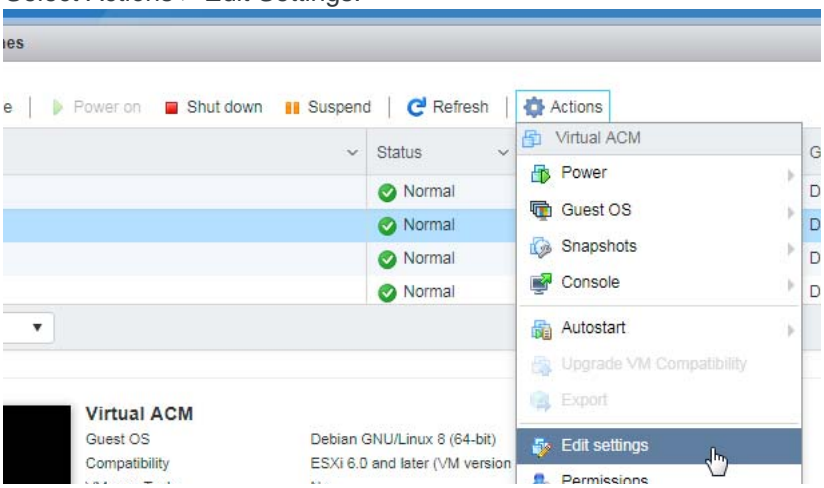


**m.** Add network adapters for the outside (eth0) interface and the inside (eth1) interface:

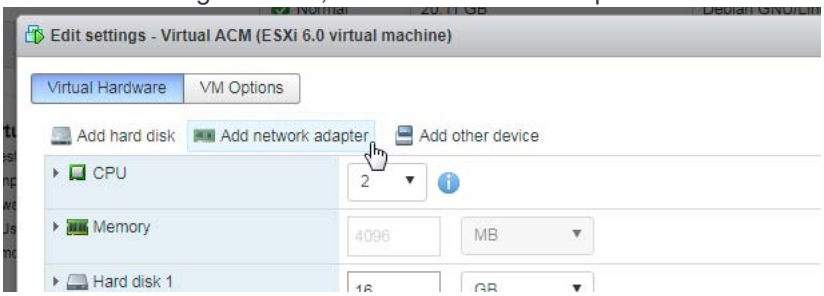
**i.** In the Virtual Machines panel, select the ACM VM that you just deployed.




**ii.** Select Actions > Edit Settings.

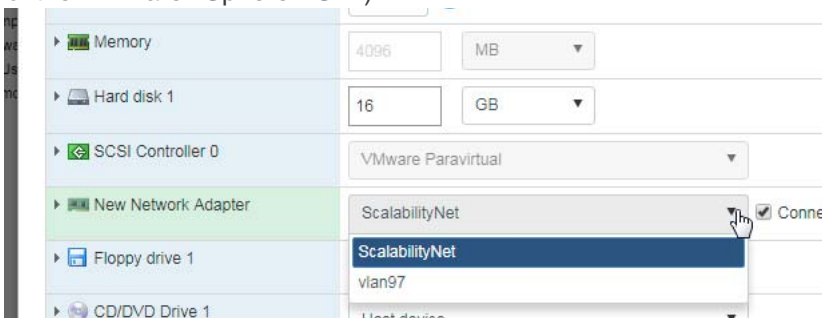



**iii.** In the Edit settings window, click Add network adapter.




**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.)

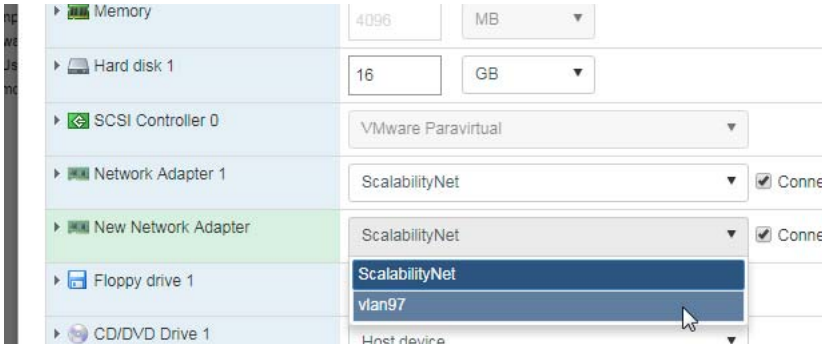



**v.** Click Save.

**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 the ACM.

# Connecting the ACM to Your Network

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

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

- AirLink devices must be able to access the ACM from the WAN. Typically, this requires that the 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 the ACM.
- The traffic between AirLink devices and the 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 the 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 1-1 on page 49).
2. At a minimum, enable the following protocols and ports for the translated address:
   - IP Protocol ESP
   - TCP/IP Port 2222
   - UDP/IP 500
   - UDP/IP 4500

If required by a customer security policy, the VPN between the AirLink gateway/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 the ACM from an Inside Device

The ACM is pre-configured with an inside network address and other information as specified in Important ACM Configuration Requirements on page 49.

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 the 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 the ACM, use the default username (*admin*) and password (*inmotion*). For example:

```
login as: admin
UNAUTHORIZED USE OF THIS SYSTEM IS PROHIBITED!
password:
   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 25 for details.*

To log out of the 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 the 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 20. |
| **delete** | Delete an attribute. | See Delete Attributes on page 21. |
| **show** | Display all pending attribute changes (add, modify, delete). | See Show Uncommitted Attribute Changes on page 21. |
| **discard** | Remove all pending attribute changes. | See Discard Uncommitted Attribute Changes on page 22. |
| **commit** | Apply all pending attribute changes to the currently running configuration. | See Apply Configuration on page 23 |
| **save** | Save the running configuration as the boot configuration. | See Save Configuration on page 23 |
| **load** | Load the ACM’s default configuration attributes. | See Restore Default Configuration on page 24 |

*Note: Attribute changes (adding, modifying, deleting, loading defaults) do not take effect on the 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 "md5"
- add a new "proposal 2" to the esp group
- add the encryption method for the new "proposal 2"

```
user@ACM1-Pro....duction# set vpn ipsec esp-group
      espgroup1 proposal 1 hash md5
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 md5
    }
+   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# 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 23.*

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

**Warning:** *This process COMPLETELY replaces the 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 the 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
```

# 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 the ACM's default hostname, use the following commands:

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

## Domain Name

To change the 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 the ACM to the enterprise network application servers (only if intermediate routers exist) use the following commands:

```
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

The 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 the ACM, <PeerID> for the peer
- Source and destination IP address of the protected traffic
- Pre-shared secret or certificate

The 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 non-FIPS and FIPS ACMs are listed in the following table.

**Table 5-1: ACM IKE/ESP Parameter Support**

| | ACM 2.0 (non-FIPS) | | ACM 2.0-FIPS | |
|---|---|---|---|---|
| **Type** | **IKE** | **ESP** | **IKE** | **ESP** |
| **Encryption** | | | | |
| aes128 | Y | Y | Y | Y |
| aes128ccm16 | | | | Y[a] |
| aes128gcm16 | | | | Y[a] |
| aes256 | Y | Y | Y | Y |
| aes256ccm16 | | | | Y[a] |
| aes256gcm16 | | | | Y[a] |
| 3des | Y | Y | | |

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

| Type | ACM 2.0 (non-FIPS) | | ACM 2.0-FIPS | |
|---|---|---|---|---|
| | IKE | ESP | IKE | ESP |
| **Hash** | | | | |
| sha1 | Y | Y | | |
| sha2_256 | Y | Y | Y | Y |
| sha2_512 | Y | Y | Y | Y |
| md5 | Y | Y | | |
| none | | | | Y[a] |
| **DH Group** | | | | |
| 1 | | | | |
| 2 | Y | Y | | |
| 5 | Y | Y | | |
| 14 | Y | Y | Y | Y |
| 15 | Y | Y | Y | Y |
| 16 | Y | Y | Y | Y |
| 17 | Y | Y | | |
| 18 | Y | Y | | |
| 19 | | | Y | Y |
| 20 | | | Y | Y |
| 21 | | | Y | Y |
| none | | Y[b] | | Y[b] |

a. When aes128ccm16, aes128gcm16, aes256ccm16, or aes256gcm16 encryption is used, hash must be none.
b. 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.

To configure IKE groups for:

- oMG/MG90 routers, and NCP Client for Windows—See Configure IKE Groups with MOBIKE (IKEv2) on page 29.
- AirLink gateways—See Configure IKE Groups with IKEv1 on page 30.

## Configure IKE Groups with MOBIKE (IKEv2)

*Note: Not all AirLink devices support IKEv2. IKEv2 is supported on oMG2000/500 and MG90 routers—see Configure IKE Groups with IKEv1 on page 30 to configure IKE groups for other AirLink devices.*

When used on supported devices, the MOBIKE (IKEv2 Mobility and Multihoming) protocol allows for fast, seamless VPN tunnel switching. Combining the oMG/MG90's intelligent WAN management with MOBIKE ensures the delivery of secure and extremely high performance mobile communications.

To enable this switching feature, both the 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 27.*

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 27 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: oMG2000/500, MG90 and NCP Client for Windows should be configured for IKEv2—see Configure IKE Groups with MOBIKE (IKEv2) on page 29.*

The following AirLink gateways support the IKEv1 protocol (IKEv2 is not supported): LS, ES, GX, RV, and MP 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 27 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
```

   - 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 27 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 gateways, optional for NCP client peers, and must not be used for oMG/MG90 routers. See Table 5-1 on page 27 for supported parameter values.

```
set vpn ipsec esp-group <ESP-GRP-NAME> proposal 10
      dh-group <Dh_group_type>
```

## VPN Peers

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

### Configure VPN Peer IDs

To configure a VPN peer ID on the 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 32, or "any".

If the <PeerID> is:

- A supported Peer ID Type from Table 5-2—The ACM creates connections for each peer, using different PSKs. This is the preferred method for oMG/MG90 routers and other AirLink gateways/routers, as it allows both the router/gateway and the client devices of the router/gateway to use the VPN tunnels.
- "any"—The ACM creates Host2LAN connections with peers of the same type (AirLink gateways/routers, or 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 not client devices that would require VPN access.
  This method is not recommended for AirLink gateways/routers, as only the router/gateway 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 sofware 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 router | WAN > VPNs > (Edit or Add)<br>Field: Auth ID | Recommended type:<br>• ESN—Router's unique serial number (<ESN>)<br>Format: @<ESN><br>Alternate types<br>• ip address<br>Format: <IP><br>• custom:<br>Format: @<custom> |

**Table 5-2: VPN Peer ID Types (Continued)**

| Peer | Location in Software | Peer ID Types |
|---|---|---|
| AirLink gateway/ router (LS, ES, GX, MP series) | VPN > VPN#<br>Field: Peer Identity Type | Recommended type:<br>• FQDN—Free-format string. User must ensure this is a unique string.<br>Format: @<FQDN><br>Alternate types:<br>• User FQDN—Free-format string. User must ensure string is unique.<br>Format: @@<USER_FQDN><br>• IP—Router's IP address<br>Format: <IP><br>*Note: If FQDN or User FQDN is used, read Main/ Aggressive Mode Configuration on page 39 for additional instructions.* |
| NCP Client for Windows | Profiles > Identities<br>Field: Type | Recommended type:<br>• Fully Qualified Domain Name<br>Format: @<FQDN><br>Alternate types:<br>• IP Address<br>Format: <IP><br>• Fully Qualified Username<br>Format: @@<User_FQDN><br>• ASN1 Distinguished Name<br>Format: <ASN1 Dname><br>(Note: Required if using certificate authentication.)<br>Not compatible with ACM:<br>• IP Subnet Address<br>• ASN1 Group Name<br>• 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 the ACM (described in Configure VPN Peer IDs on page 32.*

- 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>
```

- IKE group for the peer:

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

- IP address of 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 the 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 gateway/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 the 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 the 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 the ACM.

The default behavior in the 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

The 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 the ACM, its certificate must be signed by the same CA authority and must have the same cacert.pem certificate file that the 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 the ACM with certificates:

1. Copy the certificates into the directory: /config/auth on the 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, the ACM also supports a certificate revocation list (CRL) that explicitly lists the certificates of devices who should not be granted access to the 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 the ACM:

1. Copy the CRL file into the directory: /config/auth on the 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 the 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 source.sierrawireless.com).

# Client-side (VPN Peers) VPN Configuration

## AirLink oMG/MG90 Router Support

This section applies to AirLink oMG2000/500 and MG90. For AirLink LS, ES, and GX series gateways, and MP series routers, see AirLink Gateway/Router Support—LS, ES, GX, MP Series on page 37.

### oMG/MG90 IKE/ESP Negotiation Parameters

When using oMG/MG90 peers with the 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**

| Type | ACM 2.0 | | | | oMG | | | | MG90 | | | | Setup Requirements |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | non-FIPS | | FIPS | | non-FIPS | | FIPS | | non-FIPS | | FIPS[a] | | |
| | IKE | ESP | IKE | ESP | IKE | ESP | IKE | ESP | IKE | ESP | IKE | ESP | |
| **Encryption** | | | | | | | | | | | | | |
| aes128 | Y | Y | Y | Y | Y | Y | Y | | Y | Y | Y | Y | |
| aes128ccm16 | | | | Y[b] | | | | | | | | Y[b] | |
| aes128gcm16 | | | | Y[b] | | | | Y | | | | Y[b] | |
| aes256 | Y | Y | Y | Y | Y | Y | | | Y | Y | Y | Y | |
| aes256ccm16 | | | | Y[b] | | | | | | | | Y[b] | |
| aes256gcm16 | | | | Y[b] | | | | | | | | Y[b] | |
| 3des | Y | Y | | | Y | Y | | | Y | Y | | | |
| **Hash** | | | | | | | | | | | | | |
| sha1 | Y | Y | | | Y | Y | | | Y | Y | | | |
| sha2_256 | Y | Y | Y | Y | Y | Y | Y | | Y | Y | Y | Y | |
| sha2_512 | Y | Y | Y | Y | Y | Y | | | Y | Y | Y | Y | |
| md5 | Y | Y | | | Y | Y | | | Y | Y | | | |
| none | | | | Y[b] | | | | Y | | | | Y[b] | |
| **DH Group** | | | | | | | | | | | | | |
| 1 | | | | | | | | | | | | | |

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

| Type | ACM 2.0 | | | | oMG | | | | MG90 | | | | Setup Requirements |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | non-FIPS | | FIPS | | non-FIPS | | FIPS | | non-FIPS | | FIPS[a] | | |
| | IKE | ESP | IKE | ESP | IKE | ESP | IKE | ESP | IKE | ESP | IKE | ESP | |
| 2 | Y | Y | | | Y | | | | Y | 4.1.x[c] | | | On the ACM:<br>• Do not configure oMG peers to use DH group 18.<br>• Do not configure dh-group in esp-group proposals. |
| 5 | Y | Y | | | Y | | | | Y | 4.1.x[c] | | | |
| 14 | Y | Y | Y | Y | Y | | | | Y | 4.1.x[c] | Y | Y | |
| 15 | Y | Y | Y | Y | Y | | | | Y | 4.1.x[c] | Y | Y | |
| 16 | Y | Y | Y | Y | Y | | | | Y | 4.1.x[c] | Y | Y | |
| 17 | Y | Y | | | Y | | | | Y | 4.1.x[c] | | | |
| 18 | Y | Y | | | | | | | Y | 4.1.x[c] | | | |
| 19 | | | Y | Y | | | Y | | | | Y | Y | |
| 20 | | | Y | Y | | | | | | | Y | Y | |
| 21 | | | Y | Y | | | | | | | Y | Y | |
| none | | Y[d] | | Y[d] | | Y | | Y | | Y[d] | | | |

a. Pending release Q3 2017.
b. When aes128ccm16, aes128gcm16, aes256ccm16, or aes256gcm16 encryption is used, hash must be none.
c. ESP DH group support is available in 4.1.x. In versions <4.1, the DH group for ESP is inherited from IKE, and after a re-key, no DH group is applied to the ESP.
d. DH group 'none' is not recommended. For greater security, choose a supported ESP DH group.

# AirLink Gateway/Router Support—LS, ES, GX, MP Series

This section applies to AirLink LS, ES, and GX series gateways, and MP series routers. For AirLink oMG2000/500 and MG90 routers, see AirLink oMG/MG90 Router Support on page 36.

## ACM/AirLink (LS, ES, GX, MP Series) Setup Requirements

When using AirLink gateways/routers (other than oMG and MG90) with the ACM, some limitations apply:

- Some ACM features are not supported by 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 IKE/ESP Parameter Support**

| Type | ACM 2.0 | | AirLink | | Setup Requirements |
|---|---|---|---|---|---|
| | IKE | ESP | IKE | ESP | |
| **Encryption** | | | | | |
| aes128 | Y | Y | Y | Y | On the AirLink device:<br>• Use only AES128, AES256, or 3DES—the ACM does not support DES or None |
| aes128ccm16 | | | | | |
| aes128gcm16 | | | | | |
| aes256 | Y | Y | Y | Y | |
| aes256ccm16 | | | | | |
| aes256gcm16 | | | | | |
| 3des | Y | Y | Y | Y | |
| des | | | | | |
| none | | | Y | Y | |
| **Hash** | | | | | |
| sha1 | Y | Y | Y | Y | On the AirLink device and the ACM:<br>• Configure the peer to use only MD5 or SHA1. |
| sha2_256 | Y | Y | | | |
| sha2_512 | Y | Y | | | |
| md5 | Y | Y | Y | Y | |
| none | | | Y | Y | |
| **DH Group** | | | | | |
| 1 | | | Y | Y | On the AirLink device:<br>• Configure the device to use only DH2 or DH5.<br>On the ACM:<br>• Configure the peer to use only DH2 or DH5.<br>• Make sure the dh-group is configured in esp-group proposals |
| 2 | Y | Y | Y | Y | |
| 5 | Y | Y | Y | Y | |
| 14 | Y | Y | | | |
| 15 | Y | Y | | | |
| 16 | Y | Y | | | |
| 17 | Y | Y | | | |
| 18 | Y | Y | | | |
| 19 | | | | | |
| 20 | | | | | |
| 21 | | | | | |
| none | | | Y | Y | |

**Table 5-5: Additional ACM/AirLink Setup Requirements**

| Feature | Support limitation | Setup Requirement |
|---|---|---|
| Certificates | AirLink devices do not support certificates | On the 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 gateways/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 the 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 gateway is part of a fleet, each gateway must be configured with a unique address—modify the third and/or fourth octets for each device (modify one octet for up to 256 gateways, or both octets for 255+ gateways).
     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 gateway is part of a fleet, each gateway must be configured with a unique address—modify the third and/or fourth octets for each device (modify one octet for up to 256 gateways, or both octets for 255+ gateways).
     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 gateways/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<br>• Available only if ID Authentication ID Type is Static IP address | • Secure<br>• Best option if Static IP address is not available.<br>• All gateways/routers use the same PSK—If PSK is compromised, all gateways/routers in fleet must be configured with a new PSK. | • Not secure, PSK transmitted unencrypted in Phase 1.<br>• Gateways can use different PSKs<br>• If user accepts the security risk, this option allows for faster setup. |

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

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

(See Table 5-2 on page 32 for supported <PeerID> types and formats.)

# 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.

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

## NCP Client/ACM Setup Requirements

When using NCP Client peers with the 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 5-7: NCP Client IKE/ESP Parameter Support**

| Type | ACM 2.0 | | | | NCP Client | | | | Setup Requirements |
|---|---|---|---|---|---|---|---|---|---|
| | non-FIPS | | FIPS | | non-FIPS | | FIPS | | |
| | IKE | ESP | IKE | ESP | IKE | ESP | IKE | ESP | |
| **Encryption** | | | | | | | | | |
| aes128 | Y | Y | Y | Y | Y | Y | Y | Y | On the NCP Client:<br>• Use only AES128, AES256, or 3DES—the ACM does not support DES |
| aes128ccm16 | | | | Y | | | | | |
| aes128gcm16 | | | | Y | | | | Y | |
| aes256 | Y | Y | Y | Y | Y | Y | Y | Y | |
| aes256ccm16 | | | | Y | | | | | |
| aes256gcm16 | | | | Y | | | | Y | |
| 3des | Y | Y | | | Y | Y | | | |
| des | | | | | Y | Y | | | |
| **Hash** | | | | | | | | | |
| sha1 | Y | Y | | | Y | Y | | | |
| sha2_256 | Y | Y | Y | Y | Y | Y | Y | Y | |
| sha2_512 | Y | Y | Y | Y | Y | Y | Y | Y | |
| md5 | Y | Y | | | Y | Y | | | |
| none | | | | | | Y | | | |
| **DH Group** | | | | | | | | | |
| 1 | | | | | Y | Y | | | On the NCP Client:<br>• Configure the device to use any supported group except DH1. |
| 2 | Y | Y | | | Y | Y | | | |
| 5 | Y | Y | | | 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 | | | |
| 18 | Y | Y | | | Y | Y | | | |
| 19 | | | Y | Y | | | Y | Y | |
| 20 | | | Y | Y | | | Y | Y | |
| 21 | | | Y | Y | | | Y | Y | |
| none | | | | | | Y | Y | Y | |

**Table 5-8: 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. | Onthe NCP Client, configure to use RSA-2048. If RSA-3072 is attempted and fails, change to one of the other options. |
| Peer ID Type | ACM supports:<br>• Fully Qualified Domain Name<br>• IP Address<br>• Fully Qualified Username<br>• ASN1 Distinguished Name | On the NCP Client, use one of:<br>• FQDN (recommended)<br>• ASN1 Distinguished Name (required for certificate authentication)<br>• IP Address<br>• 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 the 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 from the ACM device page on source.sierrawireless.com.

# 6: Troubleshooting

## Upgrading to ACM 2.0

When upgrading to ACM 2.0, you must enter a name to store the image file.

To upgrade to ACM 2.0 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-2.0.0-20171021.1.iso) on the 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. “2.0.0-rc3-20171021.1”), or an alternate name of your choice, and press Enter to continue.

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

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

```
admin@ACM:~$ add system image ACM-2.0.0-20171021.1.iso
Checking MD5 checksums of files on the ISO image...OK.
...
What would you like to name this image? []: 2.0.0-20171021.1
...
```

## 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 5.3.2, Linux
      3.0.23-1-586-vyatta, i686):
  uptime: 3 days, since Nov 27 15:26:05 2015
  malloc: sbrk 409600, mmap 0, used 273032, free 136568
  worker threads: 11 of 16 idle, 5/0/0/0 working, job
      queue: 0/0/0/0, scheduled: 0
  loaded plugins: charon ldap aes rc2 sha1 sha2 md5 random
      nonce x509 revocation constraints pubkey pkcs1
      pkcs7 pkcs8 pkcs12 sshkey pem openssl fips-prf
      agent xcbc cmac hmac ctr ccm gcm curl attr kernel-
      netlink resolve socket-default stroke updown eap-
      identity eap-aka eap-md5 eap-gtc eap-mschapv2 eap-
      radius eap-tls eap-ttls eap-tnc xauth-generic
      xauth-eap tnc-tnccs error-notify certexpire
      addrblock
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 bytes_o (8 pkts, 2s
      ago), rekeying disabled
peer-any-tunnel-1{30}:   192.168.114.0/24 ===
      172.18.114.2/32
```

# 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 30.
  - If using IKEv2, use “ikev2-retransmit-timeout” and “ikev2-retransmit-tries”. See Configure IKE Groups with MOBIKE (IKEv2) on page 29.

# 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 the 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 the 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 the 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 the ACM's configuration for the peer, but does match one of the groups configured on the ACM).
  - If the peer is configured to use group_3, a tunnel will fail to establish because the 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 the ACM device page at source.sierrawireless.com.

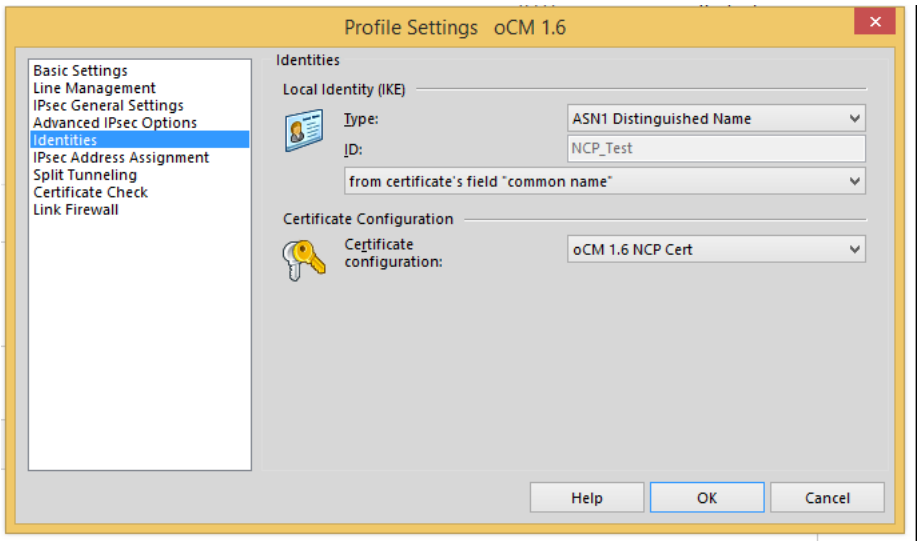



*Figure 6-1: NCP Certificate Authentication ID Type*

# A: Important ACM Configuration Requirements

A

As noted in Connecting to the ACM from an Inside Device on page 17, the information described below is required for the initial configuration of the 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 the ACM can accept connections.

**Table 1-1: 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 the 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 the ACM. The 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 the ACM and an enterprise application).

The 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 1-2: Address Space (Mobile and Enterprise) Definitions**

| Item | Note | Example |
|---|---|---|
| Mobile subnetwork(s) | Each AirLink gateway/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<br>If some mobile traffic should be allowed to bypass the tunnel, then the tunneled traffic must be specified. | 10.10.0.0/16 |