ACM 2.0 Release Notes

ACM 2.0 provides major upgrades to strongSwan and its Linux kernel, and addresses security vulnerabilities identified since the ACM 1.6 release.

The ACM 2.0 release includes both FIPS and non-FIPS versions.

ACM 2.0 is strongly recommended for all existing ACM customers.

Upgrade Requirements

Important: *Upgrade to ACM 2.0 can only be performed from ACM 1.6. Customers on previous ACM releases must first upgrade to ACM 1.6, and then upgrade from ACM 1.6 to ACM 2.0.*
Note—Upgrade can only be performed for the same ACM SKU (FIPS or non-FIPS).

ACM 2.0 can also be installed as a new instance (not upgrading from a previous ACM version) and the previous version's configuration components can be ported over.

VPN Endpoint Support

The ACM 2.0 (FIPS and non-FIPS) Release has been officially tested on the following configurations:

Platform	Endpoint (Peer) Type	Version of Embedded Software Tested
MG90	Router	MGOS 4.1.0
oMG500/oMG2000	Gateway	MGOS 3.14.6+
ALEOS-based devices (e.g. MP70, RV50, GX450, ES450)	Router & Gateways	ALEOS 4.9.0
NCP Secure Entry Client	Mobile VPN client software	• v10.10 (build 30578) • v10.11

Server Platform Support

ACM 2.0 has been tested on:
- Dell R230XL server
- VM running on VMware vSphere 6.5 (ESXi 6.5)

Note: ACM 2.0-FIPS is FIPS-compliant 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).

New Features

Virtual Machines

ACM VM is now supported on VMware vSphere 6.5 (ESXi Hypervisor).

Remote Monitoring

Remote Monitoring of ACM via Syslog and/or SNMP is now supported.

Addressed Issues

VPN

Resolved issue where source-based route would sometimes not be added to the IP table upon boot.

Resolved issue where firewall rule including reqid would be intermittently incorrect.

Resolved issue where DPD sent to wrong gateway's link would incorrectly terminate IPsec VPN.

Resolved issue where ACM would not delete old IKEv1 sessions.

Security

Several components have been patched to address security concerns reported by CVE. (A complete list of fixed CVEs is available upon request.)

Sierra Wireless 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

Corporate and product information: sierrawireless.com