ACM 2.0.1 Release Notes

The ACM 2.0.1 maintenance release includes both FIPS and non-FIPS versions.

ACM 2.0.1 is strongly recommended for all existing ACM customers.

Upgrade Requirements

Important: *Upgrade to ACM 2.0.1 can only be performed from ACM 2.0 or ACM 1.6. Customers on previous ACM releases must first upgrade to ACM 1.6, and then upgrade from ACM 1.6 to ACM 2.0.1.*
Note—Upgrade can only be performed for the same ACM SKU (FIPS or non-FIPS).

ACM 2.0.1 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.

Supported Embedded Software Versions

The ACM 2.0.1 (FIPS and non-FIPS) Release has been officially tested on the following configurations:

Embedded Software	Platform tested
MGOS 4.2	MG90
MGOS 3.15	oMG500/oMG2000
ALEOS 4.11	MP70
ALEOS 4.10	LX60
ALEOS 4.9.x	RV50, GX450 (and prior)
Tested with NCP 10.13	NCP Secure Entry Client

Server Platform Support

ACM 2.0.1 has been tested on:

- Dell R230XL server
- VM running on VMware vSphere 6.5 (ESXi 6.5)

Note: ACM 2.0.1-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).

Addressed Issues

VPN

Configuration details for “Global firewall” rules added to ACM Installation and Operations Guide to address connection timeouts on large deployments using per-VPN tunnel rules.

NCP Client

Confirmed that a new option (Enable negotiating RFC7427) in NCP Secure Entry Client for Windows 10.1x and above must be disabled to allow NCP Client to connect to ACM using a certificate. De-select the Enable negotiating RFC7427 option in
Profile Settings > Advanced IPsec Options.

Security

Addressed security issues (curl, libcurl)

- CVE-2017-8816
- CVE-2017-8817
- CVE-2018-1000122

Addressed security issues (python)

- CVE-2014-4616
- CVE-2016-5636
- CVE-2016-5699
- CVE-2016-0772

Addressed security issues (rsync)

- CVE-2017-17433
- CVE-2017-17434

Addressed security issues (sudo)

- CVE-2017-1000367

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