SIERRA WIRELESS IS NOW SEMTECH®

ACM 3.1.1

RELEASE NOTES

About ACM 3.1.1

ACM 3.1.1 has been upgraded to Ubuntu 20.04.6 LTS, and addresses security vulnerabilities.

The ACM 3.1.1 release is available in FIPS and non-FIPS configurations. Upgrading to ACM 3.1.1 is strongly recommended for all existing ACM 2.1 (FIPS / non-FIPS), ACM 2.2 (non-FIPS) and ACM 3.0 (FIPS / non-FIPS) customers.

Upgrade Methods

Important: *Direct upgrade to ACM 3.1.1 can only be performed from ACM 2.1 (FIPS / non-FIPS), ACM 2.2 (non-FIPS) or ACM 3.0 (FIPS / non-FIPS). Customers on previous ACM releases must first upgrade to ACM 2.1 (FIPS / non-FIPS) or ACM 2.2 (non-FIPS), and then upgrade to ACM 3.1.1.*

ACM 3.1.1 can be installed as:

- ACM 3.1.1 (FIPS) — Upgrade for an existing ACM 2.1 (FIPS / non-FIPS) or ACM 3.0 (FIPS)
- ACM 3.1.1 (non-FIPS) — Upgrade for an existing ACM 2.2 (non-FIPS) or ACM 3.0 (non-FIPS)
- New instance (not upgrading from a previous ACM version) and the previous version's configuration components can be ported over.

Supported Embedded Software Versions

ACM 3.1.1 is supported on the following configurations:

Platform	Embedded Software
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 version tested: 13.11 (Build 29631)
RX55, XR60, XR80, XR90	AirLink OS 4.0.23 or later

Server Platform Support

ACM 3.1.1 has been tested on VM running on VMware vSphere 7.0+ (ESXi 7.0+).

Note: New ACM installations are available as VMs running on VMware vSphere 7.

Updated VM 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.

FIPS Details

ACM 3.1.1 (FIPS) uses the following FIPS 140-2 certified packages available with Ubuntu Pro (https://ubuntu.com/security/fips) with the associated FIPS certification links:

- Linux kernel (GA) Crypto API — #4366, #4132 (AWS), #4126 (Azure), #4127 (GCP)
- OpenSSL — #4292
- libgcrypt — #3902
- StrongSwan — #4046

New Features

Operating System

[ACM 3.1] Moved to Ubuntu 20.04.6 LTS with latest packages and security fixes (released in April 2024)

[ACM 3.0] Moved from Debian to Ubuntu 20.04.5 LTS

Addressed Issues

ACM Configuration

[ACM 3.1] Resolved an issue that prevented SNMP link status reports from being received.

[ACM 3.0] Resolved an issue where, after creating an additional admin user account and committing the change, the system could not commit any additional configuration changes and would report "Failed to generate committed config".

Logging

[ACM 3.1.1] Resolved an ACM 3.1 issue that caused excessive SNMP logs.

[ACM 3.1] Resolved an issue that prevented ACM syslog (system log) files from rolling over, exhausting available disk space.

[ACM 3.0] Resolved an issue that caused TCP connections to be logged when conntrack TCP logging was not enabled.

[ACM 3.0] Resolved an issue that caused Vyatta auth.log files to grow too large and exhaust available disk space.

Security

[ACM 3.1] Several components have been patched to address security concerns reported by CVE.

(CPAN.pm)
- CVE-2023-31484

(crmsh)
- CVE-2020-35459

(curl)
- CVE-2023-28322
- CVE-2023-38545

(dnsmasq)
- CVE-2023-50387

(grub2)
- CVE-2022-2601
- CVE-2022-28734

(libxml2)
- CVE-2024-25062

(Linux kernel)
- CVE-2022-0494
- CVE-2022-1048
- CVE-2022-1652
- CVE-2022-1679
- CVE-2022-1734
- CVE-2022-1974
- CVE-2022-1975
- CVE-2022-2586
- CVE-2022-2588
- CVE-2022-28893
- CVE-2022-34918

(openssh)
- CVE-2023-38408

(openssl)
- CVE-2023-2650
- CVE-2023-5678

(perl)
- CVE-2023-47100

(squid)
- CVE-2023-5824
- CVE-2023-46728
- CVE-2023-46847
- CVE-2023-49285
- CVE-2023-49286
- CVE-2023-49288
- CVE-2023-50269

(strongSwan)
- CVE-2023-41913

(sudo)
- CVE-2023-42465

Known Issues

Dynamic DNS (DDNS)

If a network issue interrupts communication between ACMs in the DDNS cluster, the DNS data for a small number of connected gateways (~5%) may temporarily be incorrect.

The affected data recovers when IPsec tunnels change state.

Network Routing
To prevent circular route redistribution from occurring between multiple ACMs that are attached to firewalls/routers that run both OSPF and BGP: ▪ For each ACM, set up a dedicated OSPF area between ACM and its firewall router. and ▪ In the OSPF area, set up only the ACM's inside and firewall interfaces, and tag routing updates as they leave the area.
VPN
When a network issue blocks access to ACM from the gateways in a fleet, all of the gateways could attempt to establish VPN connections simultaneously when the network recovers. When this happens, if ACM cannot reach the certificate revocation server to validate certificates, only the first several VPN connection requests may succeed and the rest will time out. Whether or not this issue occurs depends on the number of gateways that are active when the network recovers. To prevent this issue from occurring, make sure ACM can reach the certificate revocation server and its DNS servers.