

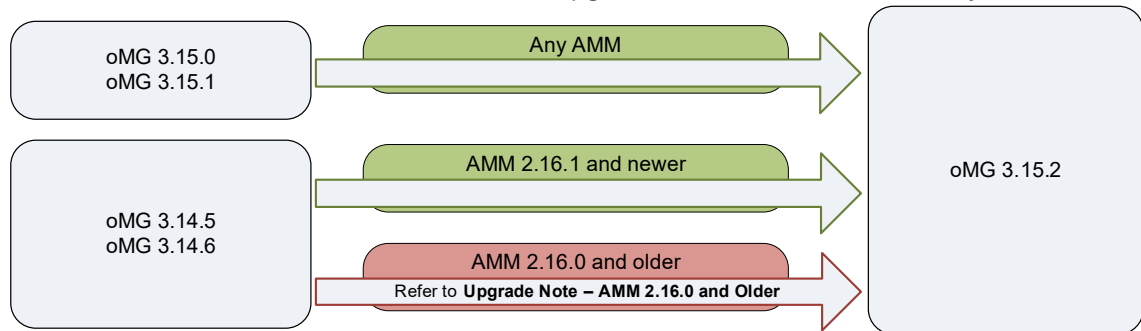
## >> oMG 3.15.2 Release Notes

oMG 3.15.2 is a critical software maintenance release for oMG2000 and oMG500 gateways. This release addresses important software issues, including security vulnerabilities.

**Important:** Customers who have not yet upgraded to oMG 3.15.x should install oMG 3.15.2. (Do not install 3.15.0 or 3.15.1.)

### Upgrade Requirements

oMG 3.15.2 can be installed as an over-the-air upgrade as shown below, or directly via USB stick.



### Upgrade Note—AMM 2.16.0 and Older

**Important:** This upgrade note applies only to customers using AMM versions AMM 2.16.0 and older, who are upgrading to oMG 3.15.2 from oMG 3.14.5 or oMG 3.14.6. This issue is resolved in AMM 2.16.1.

When upgrading to oMG 3.15.2, the application package (omg-opt-9.48804.v3.sdk4-20200319.3) must be installed twice on the oMG, as per the instructions below.

Please install oMG 3.15.2 as follows:

1. From AMM Admin/Software Distribution, choose Upgrade Gateway Software and follow the instructions to select:  
omg-core-3.15.2-20200416.1  
and  
omg-opt-9.48804.v3.sdk4-20200319.3
2. Choose Upgrade Application and follow the instructions to select:  
omg-opt-9.48804.v3.sdk4-20200319.3
3. The oMG will automatically start downloading the software on the next boot, or the download can be started immediately from the oMG LCI by selecting General > Tool > download-new-software-updates.

## Addressed Issues

### System

Resolved issue that made the gateway unable to recover from resource exhaustion resulting from extensive vehicle telemetry data collection.

### VPN

Resolved issue where VPN was unable to auto-recover after unexpected disconnection.

### WAN

Resolved issue causing cellular radio intermittent connection failures.

Resolved issue where cellular link would not appear when device was reset.

Resolved issue that allowed only one IP address to be entered for each Private Zone. Multiple comma-separated addresses can now be entered.

Improved network connection time when cellular link's APN is changed.

### Wi-Fi

Resolved issue where passenger Wi-Fi service would stop and a device reboot was required to restart it.

Resolved issue where private zone list would not display after first entry was deleted.

### AMM

Resolved issue where device could fail to establish management tunnel to AMM upon completing AMM upgrade.

Resolved issue that could cause inaccurate AMM reports (including Link Utilization).

Resolved issue that could cause oMG configuration to be out of sync with AMM.

## Resolved Security Issues

### Security

Resolved a critical LCI authentication vulnerability.

Resolved an issue where the user could bypass authentication.

Restricted remote SSH shell access to AMM only.

**Common Vulnerabilities and Exposures (CVE)®**

Addressed following CVEs:

- [CVE-2015-3310](#)
- [CVE-2015-3331](#)
- [CVE-2016-2569](#)
- [CVE-2016-2572](#)
- [CVE-2016-6321](#)
- [CVE-2016-10229](#)
- [CVE-2016-2570](#)
- [CVE-2016-3189](#)
- [CVE-2016-7117](#)
- [CVE-2016-10708](#)
- [CVE-2016-2571](#)
- [CVE-2016-3955](#)
- [CVE-2016-7798](#)
- [CVE-2017-3145](#)
- [CVE-2017-11185](#)
- [CVE-2017-13081](#)
- [CVE-2017-13088](#)
- [CVE-2017-5897](#)
- [CVE-2017-13077](#)
- [CVE-2017-13082](#)
- [CVE-2017-17740](#)
- [CVE-2017-7895](#)
- [CVE-2017-13078](#)
- [CVE-2017-13084](#)
- [CVE-2017-1000158](#)
- [CVE-2017-9022](#)
- [CVE-2017-13079](#)
- [CVE-2017-13086](#)
- [CVE-2017-1000367](#)
- [CVE-2017-9023](#)
- [CVE-2017-13080](#)
- [CVE-2017-13087](#)
- [CVE-2018-0732](#)
- [CVE-2018-10811](#)
- [CVE-2018-16152](#)
- [CVE-2018-17540](#)
- [CVE-2018-5703](#)
- [CVE-2018-14526](#)
- [CVE-2018-16229](#)
- [CVE-2018-20852](#)
- [CVE-2018-5743](#)
- [CVE-2018-16151](#)
- [CVE-2018-16230](#)
- [CVE-2019-6465](#)
- [CVE-2019-9498](#)
- [CVE-2019-9948](#)
- [CVE-2019-15166](#)
- [CVE-2019-6471](#)
- [CVE-2019-9499](#)
- [CVE-2019-10160](#)
- [CVE-2019-16056](#)
- [CVE-2019-9494](#)
- [CVE-2019-9636](#)
- [CVE-2019-11555](#)
- [CVE-2019-9496](#)
- [CVE-2019-9740](#)
- [CVE-2019-12900](#)
- [CVE-2019-9497](#)
- [CVE-2019-9923](#)
- [CVE-2019-13565](#)
- [CVE-2020-8597](#)

## Known Issues

**AMM Upgrade—Firmware installation failed: Insufficient disk space ...**

Depending on the current router configuration, the oMG 3.15.2 upgrade may fail due to insufficient disk space.

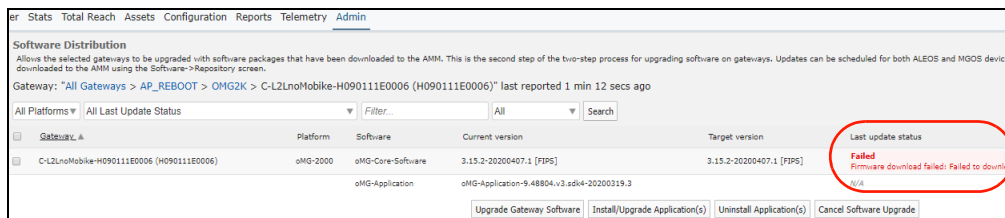
If this happens, do the following to stop the error from reoccurring:

1. In the LCI, navigate to General > Auto Software Updates.
2. Set Required Free Disk Space (MB) to 5 MB, then click Submit.
3. Navigate to General > Tools.
4. From the Command list, select the clean-local-software-update-cache and then click Execute.  
Wait until the display indicates the command has completed.
5. Try the upgrade again from AMM.
6. If the insufficient disk space error occurs again:
  - a. In the LCI, deselect “Firmware Switching Enabled” and “Firmware Download Enabled”. This will temporarily prevent the MC7354 FW images from downloading.
  - b. Click Submit.
  - c. Reattempt the upgrade.

### AMM Scheduled Upgrade—Firmware download failed: Failed to download packages.yaml.md5

An AMM scheduled upgrade may report "Firmware download failed: Failed to download packages.yaml.md5" in the following scenarios:

- Upgrade actually successful but not reported to AMM
- Upgrade failed due to unstable WAN link



The screenshot shows the 'Software Distribution' page in the AMM interface. It lists a gateway 'C-L2LnoMobile-H09011E0006' with a 'Failed' status in the 'Last update status' column. The error message is 'Firmware download failed: Failed to download packages.yaml.md5'. The interface includes tabs for 'er', 'Stats', 'Total Reach', 'Assets', 'Configuration', 'Reports', 'Telemetry', and 'Admin'. Below the table are buttons for 'Upgrade Gateway Software', 'Install/Upgrade Application(s)', 'Uninstall Application(s)', and 'Cancel Software Upgrade'.

Gateway	Platform	Software	Current version	Target version	Last update status
C-L2LnoMobile-H09011E0006 (H09011E0006)	oMG-2000	oMG-Core-Software	3.15.2-20200407.1 [FIPS]	3.15.2-20200407.1 [FIPS]	Failed Firmware download failed: Failed to download packages.yaml.md5

To resolve this:

1. Confirm whether the upgrade actually failed or succeeded—In the LCI, navigate to Status > General and check the Version and Build fields to see if they match the Target version in AMM. If they match, the upgrade succeeded, otherwise it failed.
2. In AMM, select the checkbox beside the 'failed' upgrade and then click Cancel Software Upgrade.
3. Reschedule the upgrade. When the upgrade starts,:
  - If the previous upgrade attempt actually failed, AMM reattempts the upgrade.
  - If the previous upgrade attempt actually succeeded, AMM recognizes that when it connects to the router, does not reinstall the upgrade, and sets the status to "Success  
Firmware installation finished".

### AMM Scheduled Upgrade Not Occurring

A firmware upgrade (from 3.14.5 or later) scheduled through AMM will not occur if:

- the router's software upgrade options (General > Auto Software Updates) have never been modified, and
- the router has not had a factory reset since 3.14.5 or later was installed.

If the firmware upgrade does not run as scheduled:

1. In the LCI, navigate to General > Auto Software Updates.
2. Change the Upgrade Options selection to Download Options Only.
3. Click Submit. (You do not need to leave the current screen.)
4. Change the Upgrade Options selection to Download and Apply Updates on Next Boot.
5. Click Submit.
6. Reschedule the upgrade through AMM.

## Sierra Wireless Contact Information

Sales information and technical support, including warranty and returns:

Web: [sierrawireless.com/company/contact-us/](https://sierrawireless.com/company/contact-us/)

Global toll-free number: 1-877-687-7795

Corporate and product information: [sierrawireless.com](https://sierrawireless.com)