RELEASE NOTES

VERSION 5.5.3

INTRODUCTION

Please check Upgrading firmware using the web UI for instructions on how to upgrade your device. Latest appliance software is available on the Opengear Support Software download portal.

While every effort is made to migrate your existing configuration when upgrading, we recommend that you follow the instructions on How to backup and restore the configuration BEFORE performing the upgrade.

SUPPORTED PRODUCTS

- IM7200
- CM7100
- CM7196
- ACM700x
- ACM7004-5

KNOWN ISSUES

- No known issues

CHANGE LOG

Production release: A production release contains new features, enhancements, security fixes and defect fixes.

Patch release: A patch release contains only security fixes or defect fixes for high priority issues.

5.5.3 (Oct 2026)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Improved the IPSec UI so that Phase 1 and Phase 2 ciphers and algorithms are individually selected instead of having a single dropdown with all combinations for Phase 1 only. Fields that are not applicable are hidden and explained. [OG-11251]
- Upgraded nagios-plugins to 2.4.12 and added configurations for various checks in nagios_check.xml. [OG-11771]
- Config password obfuscation support has been expanded to support PPP (dial-in/PPTP) and EAPoL. The option to enable this has been moved from the Authentication page to the System page. Additionally, the permissions for AAA conf files with secrets have been tightened. [OG-11792]
- Added webui input fields to specify Cherokee keepalive_max_requests as well as controls of per source address connection rate limit. [OG-11793]
- Added a configurable password complexity policy to the Authentication page and REST API. [OG-11795]

- Upgraded OpenSSH to 10.6p1. [OG-11875]
- Upgraded Strongswan to 6.1.0. [OG-11912]
- Upgraded libexpat to 2.9.0. [OG-11915]
- Upgraded dhcp-isc to 4.1-ESV-R16-P1. [OG-11916]
- Upgraded json-c to 0.19. [OG-11927]

Fixes

- The web server version is no longer reported in the response headers. [OG-11791]
- Fixed the race condition caused by kernel late probing the USB cellmodem to ensure its conman conns are able to be regenerated after upgrade. [OG-11871]
- Fixed the powersupply sensors' reference psmon used when writing into infod so that SNMP walk on ogPowerSupplyTable can fetch their status. [OG-11872]
- Fixed a potential heap overflow in a multipart web request. [OG-11877]

Security Fixes

- Remediation for Common Vulnerabilities and Exposures (CVEs) are included in the firmware. Please find a list of associated CVEs and their statuses in Opengear Portal.

5.5.2 (Sep 2026)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Enabled the DHCP server and IPv6 settings on the Out-of-Band/Failover interface on IM7200-24E. [OG-11753]

Fixes

- Fixed references to wwan1 that are no longer available. [OG-11628]
- Fixed cellctld holding deprecated cellmodem DBUS object path and ensured reenabling after unexpected reset. [OG-11696]
- Fixed switch detection on ACM7004-5 and IM7200. [OG-11764]
- Fixed Lighthouse VPN connection timeout, with configurable timeout support for UI and CLI enrollment. [OG-11807]
  - Set timeout to 200 seconds: 'config -s config.lhvpn.conman_test_delay=200 -r lhvpn_tunnel'
- Fixed duplicate IPv6 interface entries in the nodeDescription API response when Bridge is enabled. [OG-9153]

Security Fixes

- Patched sudo. [OG-11859]

5.5.1 (Jul 2026)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Added kernel SYN_COOKIES config option to protect against TCP SYN flood attack. [OG-11726]
- Added option for OpenVPN clients to verify server authenticity to prevent man-in-the-middle attacks. [OG-9344]

Fixes

- Fixed OpenVPN interfaces incorrectly reporting state in the SNMP NetInterfaceTable. [OG-11722]
- Fixed the WebUserStartTime in the SNMP WebUserTable. [OG-11727]
- Fixed the alarm event ID missing from entries in the SNMP CurrentAlarmTable. [OG-11729]
- Fixed RPC indexes for outlets in the SNMP RpcOutletTable. [OG-11732]
- Fixed the SNMP AlarmLogTable not reporting any autoresponse alarm log entries. [OG-11733]
- Fixed the CheckType and TriggerActions counter for UPS related state in the SNMP CheckTable. [OG-11735]
- Fixed missing CheckDeviceName values for some entries in the SNMP CheckDeviceTable. [OG-11736]
- Fixed a regression in 5.5.0 that affected the handling of user-specified cellmodem routes. [OG-11765]

Security Fixes

- Patched kernel. [OG-11734]
- Upgraded OpenSSH to 10.4. [OG-11757]
- Patched Kerberos. [OG-11762]
- Upgraded OpenVPN to 2.6.21. [OG-11762]
- Upgraded GLib to 2.88.2. [OG-11762]
- Upgraded radvd to 2.21. [OG-11762]

5.5.0 (Jun 2026)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx).

Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Fixed RADIUS Accounting packets to have NAS-IP-Address set consistently. [OG-11477]
- Fix REST-API end-point for creating users without passwords to match Web-UI behavior. [OG-11510]
- Fixed IPsec routes being lost during peer rekeying, leaving subnets unrouted despite an active tunnel. [OG-11622]
- Added support for missing user config properties to the /users REST API endpoint. [OG-11635]
- Fixed cellular instability on modems where wwan0 failed to obtain a DHCP lease (MC73xx). [OG-11659]
- Removed the unsupported dpdtimeout option for IPsec when using IKEv2 (now the default) to avoid confusion. [OG-11669]
- Removed the ability to set the password “default” or similar variants. [OG-11695]
- Upgraded BIND to 9.18.49 and enabled the “dig” tool. [OG-11708]
- Patched OpenSSL. [OG-11707]

5.4.0

This is an internal release only.

5.3.3 (May 2026)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to

have compatibility for upgrading to 5.0.0+

Enhancements

- Added support for configuring MTU on the L2 switch interface, with the value automatically applied to all member switch ports. [OG-11571]

Fixes

- Use modern ip command to setup aggregation interfaces. [OG-11581]
- Fixed 'Trusted Network' configuration changes on a cascade primary not syncing to cascade secondaries. [OG-11630]

Security Fixes

- Upgraded BIND to 9.16.48. [OG-11674]
- Upgraded GLib. [OG-11677]
- Upgraded Kerberos. [OG-11678]
- Upgraded libpng to 1.6.58. [OG-11679]
- Upgraded OpenSSL to 3.1.8. [OG-11684]
- Upgraded OpenSSH to 10.3p1. [OG-11668]
- Upgraded OpenVPN to 2.6.26. [OG-11685]
- Patched Lua. [OG-11680]
- Patched musl. [OG-11681]
- Patched Net-SNMP. [OG-11682]

5.3.2 (Mar 2026)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to

have compatibility for upgrading to 5.0.0+

Enhancements

- Improved pmshell escape handling during nested sessions. [OG-8830]
- Added /failover endpoint to support Lighthouse failover reporting. [OG-11585]
- Changed REST API session endpoints (GET/DELETE/PUT /sessions/{sid}) to return HTTP 404 for non-existent or invalid session IDs instead of HTTP 200 with “challenge-in-progress”. [OG-11595]
- Added a comprehensive list for missing carriers in India. This fixes excessive logging generated when the carrier used is not listed. [OG-11611]

Fixes

- Fixed SNMP EngineID to match exactly what is set by the user. [OG-11313]
- Fixed dd and busybox commands failing on CM7100 with the OGCS 5.x musl toolchain. [OG-11458]
- Fixed cellular firmware upgrade failures for modems that do not support storing multiple firmware images (MC7304). [OG-11518]
- Fixed an issue where harmless ntp server artifacts were left in config after a modification. [OG-11542]
- Fixed a race condition in odhcp6c that could process an IPv6 Router Advertisement on the wrong interface when multiple instances start simultaneously. [OG-11555]
- Fixed a memory leak in portmanager. [OG-11579]
- Fixed config for custom and overridden serial RPC device files. [OG-11591]
- Fixed kernel earlyprintk messages from appearing at the login prompt after device reboot. [OG-11593]
- Fixed cell health test not running when the device is configured for OOB failover mode. [OG-11596]
- Fixed an issue where ModemManager would leak memory continuously until out of memory. [OG-11600]
- Fixed the ‘-b’ option in the ‘top’ command to work as expected. [OG-11617]

Security Fixes

- Updated OpenVPN to have LZO Compression disabled by default for new tunnels. Mitigates the Voracle attack vector. [OG-9339]

5.3.1 (Dec 2025)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup

    - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Added HTTPS as default when accessing the cellfw repository: `https://ftp.opengear.com/download/cellfw/`. [OG-11502]
- Added MTU setting to IPSec tunnel configuration. [OG-11522]
- Improved portscraper to reduce writes to storage. [OG-11489]

Fixes

- Fixed an issue where adding a network host would result in extra config being left behind. [OG-11455]
- Fixed v1.9 typo in v2 REST API RAML. [OG-11534]
- Fixed DNS relay with dnsmasq installed to `/bin`. [OG-11536]
- Fixed the RSA keys' type used by webui validator to ensure they can be uploaded. [OG-11545]
- Fixed issue blocking cellular firmware updates through the REST API. [OG-11543]

Security Fixes

- Upgraded OpenSSH to 10.2p1. [OG-11492]

5.3.0 (Nov 2025)

This is a production release

NOTE

- FIPS Mode
    - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
    - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
    - Backup your configuration before attempting an upgrade to 5.x
    - After a successful upgrade, make sure to capture a new backup
    - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into

Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Features

- Added cell firmware update REST API for lighthouse [OG-11355]

Enhancements

- Added a DNS Server WebUI input field to lookup the Cellmodem's DDNS Hostname when it is unable to be resolved by the system DNS servers. [OG-11435]
- Added an input field to specify the Lighthouse Callhome MTU, which will be applied for the lhvpn1 interface of the primary enrollment. [OG-11468]
  - Note, if the primary Lighthouse server triggers a secondary enrollment to another Lighthouse server, the MTU on the lhvpn2 interface will be the default 1500.
  - The MTU of any existing enrolments can be adjusted with the following command, where "X" is 1 for the primary enrolment and 2 for the secondary one and "1200" is new MTU:
    `config -s config.lhvpn.tunnels.tunnelX.mtu=1200 -r lhvpn_tunnel`
- Improved wording around the option to save password across config erases. [OG-11446]
- Improved the handling of the Authentication REST API, allowing multiple authentication methods to have config applied in a single POST. [OG-9279]

Fixes

- Fixed Cherokee not cleaning up /var/tmp folders. [OG-11488]
- Fixed cellular modems sending and receiving SMS over the Verizon network (MC73xx). [OG-11408]
  - Users must specify `Capabilities = lte` and `Allowed Modes = 00` under:
    `Dial` -> `Internal Cellular Modem` -> `Cellmodem Capabilities and SELRAT - Advanced`
    Then re-enable the cellular modem or reboot the device.
- Fixed cellular modems dropping from the Verizon network and generating periodic ping requests over the data connection (MC73xx). [OG-11408]
  - Users can change the default settings in:
    `Dial` -> `Internal Cellular Modem` -> `Cellmodem Keepalive - Advanced`
- Fixed some incorrect hard-coded REST API versions in URLs returned by endpoints. [OG-11258]
- Fixed missing SID (session ID) field from /sessions REST API endpoint. [OG-11258]
- Fixed an issue where RADIUS requests did not include a useful NAS-IP-Address attribute. Restores the behaviour that existed before 5.2.2. [OG-11447]
- Fixed handling of unpartitioned internal USB drives on IM72xx and CM71xx devices to automatically partition, format and mount. [OG-11437]

Security Fixes

- Fixed CVEs: [OG-11495]

    - Patched OpenSSL.
    - Patched Busybox.
    - Upgraded net-snmp to 5.9.2.
    - Upgraded OpenVPN to 2.6.14.
    - Patched gLib.

5.2.4 (Jul 2025)

This is a patch release

NOTE

- FIPS Mode
    - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
    - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
    - Backup your configuration before attempting an upgrade to 5.x
    - After a successful upgrade, make sure to capture a new backup
    - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Improved efficiency when removing `-up-restarted` conns. [OG-11417]

Fixes

- Fixed IPsec tunnel over cellular modems. [OG-11415]
- Fixed web terminal when all egress IPv6 traffic is blocked on any interface. [OG-11424]
- Fixed Fail2Ban while using AAA authentication method. [OG-11426]
- Fixed OpenSSL migrations to ensure its configuration files are correct after 4.x to 5.x upgrade. [OG-11429]

Security Fixes

- Upgrade sudo package. [OG-11428]

5.2.3 (Jun 2025)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Fixed the ability to correct Verizon APN settings during data connection for cellular modems. [OG-11343]
- Fixed cell-fw-update to recover from the low-power mode should it fail during cellmodem firmware update. [OG-11344]
  - Added a button on the dialin page to remove selected carriers.
- Fixed an issue where HTML special characters could not be used in CSR fields (Organization, Organization Unit). [OG-11346]
- Fixed cellmodem connection issues with the wwan1 interface and the cdc-wdm1 control device (MC74xx). [OG-11361]
- Fixed openvpn server not binding to a given address or DNS hostname. [OG-11376]
- Fixed Fail2Ban regex to capture ssh login failures from the syslog. [OG-11389]
- Fixed minor IPSec duplicate configuration issue. [OG-11390]
- Fixed full-tunnel ipsec default route metric. [OG-11377]
  - A new Right Metric option has been added to the IPsec configuration page for modifying the metric used for routes to the peer or peer subnet if specified. Defaults to 100.

Security Fixes

- Upgrade OpenSSH to version 10.0p1. [OG-11394]

5.2.2 (May 2025)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Added logging of failed conman start and stop commands. [OG-11319]

Fixes

- Fixed cellmodem responding to external ICMP requests after disconnection (EM7565 and MC74xx). [OG-11333]
- Fixed issue with IPSec host-to-host or subnet-to-host configurations. [OG-11296]
- Fixed VPN routes not being added when configured on the WebUI (with Interface == None). [OG-11367]
- Fixed missing dos2unix package (CM71xx and CM7196a). [OG-11370]
- Fixed an issue where deleting all IPSec tunnels did not flush route table 220. [OG-11371]
- Fixed the bond interface going down once any enslaved interface is dropped (a regression introduced in 5.2.1 by OG-11298). [OG-11368, OG-11369]

Security Fixes

- Upgrade pam_radius to version 3.0.0. [OG-11336]
  - A new “Require Message-Authenticator” option has been added to RADIUS settings to mitigate BlastRADIUS attacks. It must be enabled manually, as it’s off by default after a config erase.
  - Added BlastRADIUS mitigation endpoint to REST API. [OG-11352]
- Upgrade OpenSSH to version 9.9p2. [OG-11335]

5.2.1 (Feb 2025)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
  - Backup your configuration before attempting an upgrade to 5.x
  - After a successful upgrade, make sure to capture a new backup
  - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Added support for the external EMD32 Environmental Monitor (EMD). [OG-11182] [OG-11204]
  - EMD32 is interchangeable with EMD5000
  - EMDs connect to the RS232 serial port via the EMD adapter cable.

Fixes

- Fixed cellmodem connection failure on /dev/cdc-wdm1 by disabling RMNET usb endpoints (MC73xx). [OG-11173]
- Fixed an issue where RPC status indicators displayed incorrect status and colour after upgrading to 5.1.1. [OG-11287]
- Fixed the race condition to set WAN MTU while bonding is enabled.[OG-11298]
- Fixed ez-ipupdate being restarted too quickly due to wrong user configurations of dyndns. [OG-11308]
- Fixed USB provisioning (ZTP) (IM72xx). [OG-11311]
- Fixed handling of duplicate conns/groups in conman config. [OG-11315]
- Fixed default self signed openssl certificates not being automatically renewed. [OG-11329]
- Fixed dashboard configuration to sanity check the number of widgets. [OG-11330]
- Fixed the description of the first USB stick in the configuration. [OG-11331]
- Fixed ability to connect to some Aruba and Cisco USB consoles by adding cdc_acm driver back (CM71xx). [OG-11188]

Other

- CDMA bands will now be disabled on -LMV SKUs using MC7354 cell modem modules. [OG-11297]
    - To override this behavior and continue using legacy CDMA bands run:
      `config -s config.cellmodem.enable_cdma=on`
      `/etc/scripts/cell-carrier`
    - The second command will be automatically run in time, this sequence of commands will ensure the effect is immediate.

5.2.0 (Nov 2024)

This is a production release

NOTE

- FIPS Mode
    - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
    - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- Backup configuration files with a different major version than the current firmware version will no longer be applied.
    - Backup your configuration before attempting an upgrade to 5.x
    - After a successful upgrade, make sure to capture a new backup
    - If there are any upgrade issues, revert back to 4.x and re-apply the 4.x backup config
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Feature

- IPSec IKEv2 Support. [OG-11195]
    - Add IKEv2 to allow for multiple subnets and is also more secure and recommended for Key Exchange.
    - Adds the “IKE Version” option to the UI with the available values: Auto, IKEv1, and IKEv2.
        - Connections marked with ‘Auto’ will use IKEv2 when initiating, but accept any protocol version when responding.
    - Add back the 4x ipsecX interface.
        - A virtual ‘ipsecX’ interface where ‘X’ is the tunnel IPsec number as it appears in config.
        - Uses VTI and user space.
        - Allows for interface based routing over policy based in the firewall.
        - Allow for the Forwarding and Masquerading UI page to forward between IPSec

and other interfaces.
    - IPSec initiator will now restart on a responder ipsec restart command.
    - Correct phase 2 Perfect Forward Secrecy of keys (PFS) behavior.

- Added IPSec missing DH groups. [OG-10991]
    - NIST Elliptic Curve Groups.
        - `ecp192-ecp224-ecp256-ecp384-ecp521`
    - Available for phase 1 (Negotiable only) and phase 2.
        - For individual selection of both phase 1 or phase 2 ciphers, its recommend to use the Custom Tunnel Options and this can override any previous settings in the UI.
        - For example (Option name = Argument):
          For phase1:
          `ike = <encryption_alg>-<integrity_alg>[-<prf>]-<dh_group>`
          For phase2:
          `esp = <encryption_alg>-<integrity_alg>-<dh_group>`
          Or:
          `ah = <integrity_alg>[-<dh_group>]`
            - e.g. `ike = aes256gcm12-sha256-modp4096`
        - To utilize the AEAD (Authenticated Encryption with Associated Data) algorithms that can't be combined with classic encryption ciphers in the same proposal, the Custom Tunnel Option is also recommended.

Enhancements

- Added handling for bearers inactive timeout threshold (IM72xx). [OG-10986]
    - Some carriers may have adopted bearer's inactive timeout threshold, and if the ipv6 connection stays idle (no application-driven traffic) the bearer connection may be dropped. Although the cellmodem could reconnect and obtain new ipv6 addresses, the link is not usable.
    - To avoid such situations, use the following two config variables to enable the pinging of cellmodem's gateway's ipv6 link-local address to keep the connection alive:
      `config -s config.cellmodem.ipv6.keepalive.enabled=on`
      `config -s config.cellmodem.ipv6.keepalive.threshold=900`
    - The first variable is not needed for the Verizon network (since this "keepalive" feature is automatically enabled for it).
    - The second variable, if unset, defaults to 3600 seconds, or 1 hour
- Fixed issues with DNS over IPv6 when another interface is configured as IPv4. [OG-11203]
    - DNS, Media, MTU and Serial Port Aliases also apply to IPV6 Settings and are now grouped together and located after the IPv4 and IPv6 settings.
- Add missing help info in the web UI for custom OpenVPN tunnels. [OG-11157]

Fixes

- Fixed an issue where having a USB ZTP image parameter prevented the script or lighthouse parameters from being used. [OG-11156]
- Fixed an issue where ACM devices would have high CPU utilization when /var/mnt/storage.nvlog was not mounted. [OG-11164]
    - If the behaviour is present on IM/CM products, the user will need to specify volume format in config for the storage media.
- Fix issue with link speed/duplex not being set on IM72xx OOBFO interface. [OG-11192]
- Fixed jumbo frame drops when the path MTU is larger than the TX checksum offload limit of the Ethernet controller (1600 bytes) (IM72xx). [OG-11213]

- Fixed static route behavior. [OG-11241]
- Fixed an issue where crontab stored files in volatile storage instead of /etc/config/crontab.'user' as 4.x does. [OG-11242]
- Fixed /etc/scripts/cellmodem-power not working as expected (MC7430). [OG-11244]
- Fixed IPv6 addresses accruing (MC7354). [OG-6488]
- Fixed IPv6 configuration disallowed error for the cellmodem when it is not supported by the carrier [OG-11250]
- Fixed redundant invocation of conman_status when checking if cellmodem is configured as the failover interface. [OG-11278]
- Fixed web terminal to serial ports 502 Bad gateway error [OG-11280]
- Fixed web terminal to serial ports intermittently hangs on user input [OG-11276]
- Fixed snmpd restarting unnecessarily when an interface's override ifDescr token is used. [OG-11289] [OG-11274]

Other

- Backup configuration files with a different major version than the current firmware version will no longer be applied. [OG-11257]

5.1.1 (Oct 2024)

This is a patch release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Added XFRM state and policies, and IP tunnel info to the support report. [OG-11172]

Fixes

- Fixed client side SFTP support. [OG-11221]
- Fixed issues with IPsec by setting system routing rules at a fixed and known priority. [OG-11183]
- Fixed an issue where setting RADIUS to MSCHAPv2 would sometimes add PAP headers to

the request. [OG-11152]
- Fixed an issue that prevented port sessions to disconnected USB ports from being cleaned up as expected. [0G-11044]
- Fixed an issue where SFP interfaces were not allowed to use 1000base Tx-FD when auto-negotiation fails. [OG-11161]
- Fixed an issue where the dashboard widget settings would be overwritten with defaults until the widget layout is saved. [OG-11163]
- Fixed an error when updating user passwords with the API when there are multiple local users. [OG-11191]
- Fixed infod high CPU usage while generating support report. [OG-11162][OG-11239]

Security Fixes

- Patched OpenSSH. [OG-11189]
- Patched libexpat. [OG-11219]

5.1.0 (Aug 2024)

This is a production release

NOTE

- FIPS Mode
  - OpenSSL key sizes of 1024 are no longer permitted by the FIPS provider. All 1024 key lengths (any user uploaded or default Web SSL CSRs) will be migrated / generated to a 2048 bit key length.
  - The OpenSSL MD5 digest is no longer available in FIPS mode on 5.1.0+
- This release includes security changes that impact a case where a Lighthouse VPN server certificate can be SHA-1 signed and will prevent the Console Server device enrolling into Lighthouse. Please refer to https://portal.opengear.com/customerservice/s/article/Lighthouse-VPN-Certificate-Upgrade-Failure for additional details.
- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Features

- Added FIPS support.
  - The OpenSSL FIPS provider version is pinned at 3.0.9 which is certified as compliant with FIPS 140-2. [OG-11065]
- Added NAT64 support. [OG-10990]
- Added SNMP configuration to set interface descriptions. [OG-11113]
- Added Remote Authentication AAA connection timeout configuration. [OG-11142]

Enhancements

- Added support for Panduit G5 PDU for dynamic outlet detection. [OG-11079]
- Enabled IPSec updown to run a custom script on up/down and enable a custom script to

be run when the cellular interface gets an IP address. [OG-11166]
    - Enabled the IPVTI kernel module.

Fixes

- Fixed a failure to enrol 5.x node with Lighthouse driven enrollment in IPv6 only setup. [OG-11132]
- Fixed issue preventing SMS sending (IM72xx-LMV). [OG-11015]
- Fixed IPv6 serial port aliases failing to apply when IPv4 is not configured. [OG-11159]
- Fixed inconsistent WAN routes metrics. [OG-11122]

5.0.5 (Jun 2024)

This is a patch release

NOTE

- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Fixes

- Fixed cellmodem bearers having issues disconnecting when using some carrier's APN (MC7430). [OG-11063]
- Fixed frequent SNMP `No such file or directory` messages in syslog. [OG-11070]
- Fixed default credentials not working after upgrade to 5.0.0+ (rev6 IM72xx). [OG-11101]
- Fixed cherokee and sshd warnings about missing SSL certificate after config erase. [OG-11102]
- Fixed setting up crontab.root after config erase. [OG-11103]
- Fixed cell and dormant failover static routes not installing until failover occurs. [OG-11105]

5.0.4 (May 2024)

This is a patch release.

NOTE

- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Fixes

- Fixed displaying the name of current active carrier on cellmodem (MC73xx). [OG-11057]
- Fixed cellmodem sim2sim failover. [OG-10258]
- Fixed a false-positive error message when groups are initialized at startup. [OG-11054]
- Fixed RADIUS + PAP appending garbage characters to passwords. [OG-11058]
- Fixed Statistics > Cellular page failing to display preferred firmware/carrier. [OG-11062]
- Fixed ipsec configurator segfault when cellular modem is enabled but has failed to obtain an IP address from the bearer. [OG-11064]

Other

- Removed WiFi support as of 5.0.0 (IM72xx).
- EOL notice for WiFi was given in April of 2019 and has now been discontinued.
- Remove support for FIPS 140-2 as of 5.0.0. If using FIPS mode, it is recommend to remain on a previous version of 4.x.x.
- Remove SDT Connector as of 5.0.0. [OG-9717]

5.0.3 (Apr 2024)

This is a patch release.

NOTE

- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Fixes

- Fixed the `sfp_info` command causing issues with the GPIO line when enabling the SFP module on ACM7004-5. Also sometimes triggered by generation of the support report. [OG-11001]
  - Workaround is to reboot the device
  - Or run `gpioset 4 22=0`
- Fixed CLI session timeout not working. [OG-11047]
- Fixed TFTP not working. [OG-11048]
  - Workaround is to remove the following line
    `69 stream udp nowait root /bin/tftpd /var/mnt/storage.nvlog/tftpboot`
    from `/etc/config/inetd.conf` and restart `inetd`
  - Or run `sed -i '/^69 stream/d' /etc/config/inetd.conf; killall inetd`
- Fixed early failure when attempting to resolve an unreachable Lighthouse external IP address. Allowed additional external IPs to be attempted. [OG-11012]
- Fixed cellctld segfault while accessing bearer's ipv6 configuration. [OG-11055]
- Fixed ModemManager regex initialisation error. [OG-10967]

Other

- Removed WiFi support as of 5.0.0 (IM72xx).
  - EOL notice for WiFi was given in April of 2019 and has now been discontinued.

- Remove support for FIPS 140-2 as of 5.0.0. If using FIPS mode, it is recommend to remain on a previous version of 4.x.x.
- Remove SDT Connector as of 5.0.0. [OG-9717]

5.0.2 (Mar 2024)

This is a patch release.

NOTE

- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Improved wording around Modem Watchdog threshold function. [OG-6855]
- Improved cell-modem interface determinism. [OG-8110]
- Improved clarity of disabled interfaces in ogNetInterfaceTable. [OG-11004]
- Restored lsusb behaviour from OGCS 4. [OG-10987]

Fixes

- Fixed a potential bootloop issue when upgrading from version 4.x.x to 5.x.x. (ACM700x) [OG-10994]
- Fixed inconsistent system state with wrong PID in conman.pid. [OG-3551]
- Fixed auto-response starting multiple network event triggers. [OG-8529]
- Fixed ICMPv4 echo-requests to a cellmodem address still receiving responses once the connection has been disconnected. [OG-10258]
- Fixed a bug where the correct SIM slot is not confirmed to be active before modifying profiles. [OG-10522]
- Fixed console output not mapping newlines. [OG-10955]
- Fixed power supply values not being updated in SNMP OIDs. [OG-10968]
- Fixed SNMP displaying duplicate PSU sensors. [OG-10972]
- Fix the Delay Config Commits feature preventing the re-generation of configuration files after upgrade. [OG-11007]
- Fixed a bug in snmpstatusd to ensure the ogEmdTable OID may be fetched correctly. [OG-10989]
- Fixed the modeSettings documentation in the RAML. [OG-10985]
- Fixed bug preventing access to cascaded device ports. [OG-11014]

Other

- Added missing radvd package. [OG-10988]
- Removed “Cellmodem MTU” field from “Enable Dial-Out” page. [OG-9281]
- Removed WiFi support as of 5.0.0 (IM72xx).
    - EOL notice for WiFi was given in April of 2019 and has now been discontinued.
- Remove support for FIPS 140-2 as of 5.0.0. If using FIPS mode, it is recommend to remain on a previous version of 4.x.x.

- Remove SDT Connector as of 5.0.0. [OG-9717]

5.0.1 (Feb 2024)

This is a patch release.

NOTE

- In version 5.0.0 a Linux kernel update was introduced. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.
- Added minimum required versions before upgrade to 5.0.0+ (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0+

Enhancements

- Sierra Wireless RRC logging now occurs via QCDM. [OG-10920]
- SSH keys may be removed using a new delete API. [OG-10822]
- Updated Statistics Failover & Out-of-Band page to show IP address. [OG-8543]

Fixes

- Fixed USB serial ports not appearing (CM71xx). [OG-10960]
- Fixed Custom WAN MTU causing eth0 routes to disappear. [OG-10930]
- Fixed cell-fw-update attempting to update already up-to-date firmware. [OG-10929]
- Fixed sysObjectID OID showing ogIM72xx (CM71xx). [OG-10928]
- Fixed corrupted support reports (CM71xx). [OG-10927]
- Fixed connection refused error for SSH to port 30xx. [OG-10922]
- Fixed modem-watchdog failing to find cellmodem interface. [OG-10903]
- Fixed StrongSwan IPSec phase2 not occuring. [OG-10902]
- Fixed missing password parameter from /auth endpoint for TACACS. [OG-10859]
- Fixed inconsistent GET users/{$id} results. [OG-10821]
- Fixed https redirect with HSTS enabled. [OG-10815]
- Fixed overly strict cellular username field disallowing certain characters. [OG-10734]
- Fixed restricting access to PDU outlets via group permissions breaking access to subsequent PDU outlets. [OG-10703]
- Fixed iptable entry not being created when forwarding between the same interface. [OG-10634]
- Fixed monitored/remote UPS connection not being removed. [OG-10613]
- Fixed RPC Status page Outlet tabs changing inconsistently. [OG-10531]
- Fixed IPv6 DNS servers on cellmodem populating wwanX.dhcp rather than wwanX.dhcp6. [OG-10179]
- Fixed erroneous errors during the transfer of the main RSA public key to the cascaded nodes using SCP. [OG-9798]
- Fixed multiple DHCP servers on various interfaces resulting in conflicts within the dhcpd.conf file. [OG-9236]
- Fixed GPS Fix Frequency Web UI notation and functionality. [OG-8183]
- Fixed DHCP server logs polluting syslog before LAN interface is up. [OG-7503]
- Fixed overly permissive file permissions for /etc/config/hosts. [OG-10824]
- Fixed issue where script templates could not be applied from Lighthouse. [OG-10934]

- Patched PAM TACPLUS. [OG-10943]
- Patched StrongSwan. [OG-10945]
- Patched OpenSSL. [OG-10938]
- Patched PCRE2. [OG-10939]
- Patched OpenVPN. [OG-10941]
- Patched Sudo. [OG-10946]
- Patched PAM KRB5. [OG-10942]
- Patched Netcat. [OG-10940]
- Patched OpenSSH. [OG-10944]

Other

- Removed WiFi support as of 5.0.0 (IM72xx).
    - EOL notice for WiFi was given in April of 2019 and has now been discontinued.
- Remove support for FIPS 140-2 as of 5.0.0. If using FIPS mode, it is recommend to remain on a previous version of 4.x.x.
- Remove SDT Connector as of 5.0.0. [OG-9717]

5.0.0 (Nov 2023)

This is a production release that includes a Linux kernel update. It is recommended to conduct a thorough validation test of this software update on a limited number of devices prior to a full-scale rollout. This best practice ensures compatibility and smooth integration with your specific environment.

NOTE

- Added minimum required versions before upgrade to 5.0.0 (CM71xx and IM72xx). Devices must be upgraded to a version starting from 4.13.3 to any later 4.13.x release to have compatibility for upgrading to 5.0.0

Features

- Upgraded the Linux kernel, move to modern security standards and utilize a well supported standard C library.
    - Upgraded Linux Kernel from 3.10.0 to 5.17.0.
    - Upgraded OpenSSL from 1.0.1u to 3.1.2 (Enables TLSv1.3 and disables 1.0 and 1.1).
    - Upgraded OpenSSH from 7.7 to 9.5p1 (adds host-key algorithms: rsa-sha2-512 (2048-bit), rsa-sha2-256 (2048-bit)).
    - Upgraded OpenVPN from 2.4.6 to 2.6.2 (supports OpenSSL 3.0, TLS v1.3 and enforces stricter TLS, cipher selection, and modern security standards).
    - Changed Openswan U2.6.37/K to Strongswan 5.9.11 (Added authentication algorithm options for IKE and ESP/AH cipher suites sha256 and sha512).

Enhancements

- Update output of ifconfig and Statistics UI page due to updated kernel.
- Upgrade IPsec, implementation changed to Strongswan from Openswan. [OG-9444]
    - Aggressive mode now defaults to off for security reasons.
    - Strongswan does not present the “ipsec0” interface in ifconfig output. This has no effect on functionality, however IPsec tunnels may still be queried through CLI with “ipsec status”.
    - When overriding the default ciphers, perfect forward secrecy is now activated by

providing Diffie-Hellman groups in the Phase 2 ESP/AH ciphers.
    - Added authentication algorithm options for IKE and ESP/AH cipher suites sha256 and sha512.
    - Renamed dh22, dh23, and dh24 Diffie-Hellman groups to modp1024s160, modp2048s224, modp2048s256.
    - The keywords “leftsubnets” and “rightsubnets” are now “leftsubnet” and “rightsubnet” and limited to a single subnet.
    - The “leftsourceip” and “rightsourceip” options were cleared and are now derived from the leftsubnet and rightsubnet fields and are no longer required for LAN or Cellular tunnels
- Change DNS Resolver IPv4/IPv6 preference configuration. [OG-10316]
    - This has moved to /etc/config/resolvpref.conf from /etc/gai.conf.
- Update micro SD card to normalized path. [OG-10313]
    - config.storage.sd.device has been normalized to /dev/mmcblk0p1. This path will be update automatically during the upgrade.
- Update REST API version to v1.8
    - SDT configuration was removed from the REST API, so the latest API version has been incremented.
- Add syslog warning message for cases where the system clock is out of a pre-set range which likely indicates a bad Real Time Clock (RTC) battery. [OG-10876]
- Reduce PHY emissions. [OG-10798]
- Enhancement to allow applying a config backup between IM7200-24E and non- IM7200-24E devices. [OG-10895]

Fixes

- Fix protocol identifiers in inetd.conf, tcp6 and udp6 changed to tcp46 and udp46. [OG-9291]
- Fix some classes of error messages being un-logged.
- Error messages will now appear on the console when “config.console.debug=on”.
- Fix ethernet routes not being removed when aggregation is enabled.
- Fix an issue where the MC7455 modem would load Verizon firmware instead of AT&T, even when configured for AUTO-SIM with an AT&T SIM card inserted. [OG- 10607]
- Fix an error when checking for cellular firmware updates. [OG-10651]
- Fix issues of internal services restarting when logging facilities are used. [OG- 10738]
- Upgrade IEEE 802.1x (EAPOL) to use PEAP-MD5 instead of PEAP-MSCHAPv2 which utilises a weak cipher. [OG-10466]
- Fix REST API PATCH request method for serialPorts endpoint. [OG-10693]
- Fixed an issue where autoresponse could not match regular expressions in multi- line SMSes by replacing ” with ’ ’ in incoming SMS messages before applying regular expressions. [OG-10778]

Other

- Remove WiFi support (IM72xx).
    - EOL notice for WiFi was given in April of 2019 and has now been discontinued.
- Due to kernel changes, the output of ifconfig is slightly different. This results in changes to the Statistics UI page and may break existing scripts that make use of the device IP.
- Remove support for FIPS 140-2. If using FIPS mode, it is recommend to remain on a previous version of 4.x.x.
- Remove FAT32 mount option “-o sync”, consider replacing with “-o flush”. [OG- 9844]
- Remove all options from lsusb.
    - Output may be filtered using grep.

- Remove SDT Connector. [OG-9717]
- Remove Network Host Permitted Services and Host Logging.
- Router Throughput Performance Using Iperf3 With 128KB Buffers:
    - Bandwidth Results With Bridging Enabled ACM7000, CM7100: 550 Mbps IM7200: 700 Mbps
    - Bandwidth Results With IP Forwarding Enabled ACM7000, CM7100: 430 Mbps IM7200: 600 Mbps